

DOCKET NO.: 267285US90PCT

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

IN RE APPLICATION OF: Yusuke HISADA, et al.

SERIAL NO.: NEW U.S. PCT APPLICATION

FILED: HEREWITH

INTERNATIONAL APPLICATION NO.: PCT/JP04/09446

INTERNATIONAL FILING DATE: July 2, 2004

FOR: REMOTE-ACCESS VPN MEDIATING METHOD AND APPARATUS

**REQUEST FOR PRIORITY UNDER 35 U.S.C. 119**  
**AND THE INTERNATIONAL CONVENTION**

Commissioner for Patents  
Alexandria, Virginia 22313

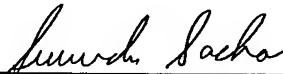
Sir:

In the matter of the above-identified application for patent, notice is hereby given that the applicant claims as priority:

<b><u>COUNTRY</u></b>	<b><u>APPLICATION NO</u></b>	<b><u>DAY/MONTH/YEAR</u></b>
Japan	2003-271202	04 July 2003

Certified copies of the corresponding Convention application(s) were submitted to the International Bureau in PCT Application No. PCT/JP04/09446. Receipt of the certified copy(s) by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

Respectfully submitted,  
OBLON, SPIVAK, McCLELLAND,  
MAIER & NEUSTADT, P.C.



Masayasu Mori  
Attorney of Record  
Registration No. 47,301  
Surinder Sachar  
Registration No. 34,423

Customer Number

**22850**

(703) 413-3000  
Fax No. (703) 413-2220  
(OSMMN 08/03)

PCT/JP 2004/009446

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

Rec'd PCT/PTO 08 MAR 2005  
28.07.2004

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日  
Date of Application: 2 0 0 3 年 7 月 4 日

出 願 番 号  
Application Number: 特 願 2 0 0 3 - 2 7 1 2 0 2

[ST. 10/C]: [ J P 2 0 0 3 - 2 7 1 2 0 2 ]

出 願 人  
Applicant(s): 日 本 電 信 電 話 株 式 会 社

REC'D 16 SEP 2004

WIPO

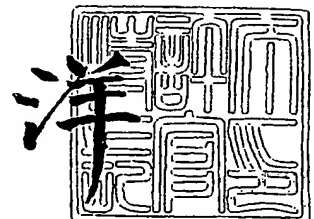
PCT

PRIORITY DOCUMENT  
SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH  
RULE 17.1(a) OR (b)

2 0 0 4 年 9 月 2 日

特許庁長官  
Commissioner,  
Japan Patent Office

小 川



出証番号 出証特 2 0 0 4 - 3 0 7 8 7 4 1

【書類名】 特許願  
【整理番号】 NTTH147644  
【提出日】 平成15年 7月 4日  
【あて先】 特許庁長官 殿  
【国際特許分類】 G06F 17/00  
【発明者】  
    【住所又は居所】 東京都千代田区大手町二丁目 3 番 1 号 日本電信電話株式会社内  
    【氏名】 久田 裕介  
【発明者】  
    【住所又は居所】 東京都千代田区大手町二丁目 3 番 1 号 日本電信電話株式会社内  
    【氏名】 鶴岡 行雄  
【発明者】  
    【住所又は居所】 東京都千代田区大手町二丁目 3 番 1 号 日本電信電話株式会社内  
    【氏名】 小野 諭  
【特許出願人】  
    【識別番号】 000004226  
    【氏名又は名称】 日本電信電話株式会社  
    【代表者】 和田 紀夫  
【代理人】  
    【識別番号】 100073760  
    【弁理士】  
    【氏名又は名称】 鈴木 誠  
【手数料の表示】  
    【予納台帳番号】 011800  
    【納付金額】 21,000円  
【提出物件の目録】  
    【物件名】 特許請求の範囲 1  
    【物件名】 明細書 1  
    【物件名】 図面 1  
    【物件名】 要約書 1

**【書類名】 特許請求の範囲****【請求項 1】**

IP ネットワークにVPN クライアント装置及びVPN ゲートウェイ装置が接続され、VPN ゲートウェイ装置により管理されるローカルエリアネットワークに通信装置が接続され、前記 IP ネットワークに接続された任意のVPN クライアント装置と、VPN ゲートウェイ装置、及び、VPN ゲートウェイ装置に管理されるローカルエリアネットワークに接続された任意の通信装置との間のトンネリングプロトコルによるリモートアクセスVPN を実行するシステムにおけるリモートアクセスVPN 仲介方法であって、

前記 IP ネットワーク上に仲介装置を設け、前記VPN ゲートウェイ装置から前記通信装置に割り当てられたプライベートIP アドレスを示す情報（以下、アクセスコントロールリスト）を前記仲介装置に送信し、該仲介装置で記憶することを特徴とするリモートアクセスVPN 仲介方法。

**【請求項 2】**

前記仲介装置と前記VPN ゲートウェイ装置との間の通信路を暗号化して、前記VPN ゲートウェイ装置からアクセスコントロールリストを前記仲介装置に送信することを特徴とする請求項 1 記載のリモートアクセスVPN 仲介方法。

**【請求項 3】**

前記仲介装置は、前記VPN ゲートウェイ装置を認証し、認証に成功した場合に、前記VPN ゲートウェイ装置により送信されたアクセスコントロールリストを記憶することを特徴とする請求項 1 もしくは 2 記載のリモートアクセスVPN 仲介方法。

**【請求項 4】**

前記仲介装置は、前記VPN クライアント装置から前記VPN ゲートウェイ装置に割り当てられたIP アドレスの検索要求を受信したなら、前記VPN クライアント装置が前記VPN ゲートウェイ装置のアクセス権限を有するかどうか検証し、アクセス権限を有する場合に限り、

- (1) アクセスコントロールリストを参照して、通信装置に割り当てられたプライベートIP アドレスを取得し、
  - (2) ドメインネームサーバを検索してVPN ゲートウェイ装置に割り当てられたIP アドレスを取得し、
  - (3) VPN クライアント装置とVPN ゲートウェイ装置との間の認証に用いる共通鍵を生成し、
  - (4) 仲介装置とVPN クライアント装置との通信路を暗号化して、VPN ゲートウェイ装置のIP アドレス、通信装置のプライベートIP アドレス及び共通鍵をVPN クライアント装置に送信し、
  - (5) 仲介装置とVPN ゲートウェイ装置との通信路を暗号化して、VPN クライアント装置のIP アドレス及び共通鍵をVPN ゲートウェイ装置に送信する、
- ことを特徴とする請求項 1 乃至 3 記載のいずれか 1 項に記載のリモートアクセスVPN 仲介方法。

**【請求項 5】**

VPN クライアント装置は、SPKI 方式に従って証明書を発行し、前記証明書を受信した他のVPN クライアント装置が前記仲介装置に対して、前記VPN ゲートウェイ装置に割り当てられたIP アドレスの検索要求を送信することを特徴とする請求項 4 記載のリモートアクセスVPN 仲介方法。

**【請求項 6】**

IP ネットワークにVPN クライアント装置及びVPN ゲートウェイ装置が接続され、VPN ゲートウェイ装置により管理されるローカルエリアネットワークに通信装置が接続され、前記 IP ネットワークに接続された任意のVPN クライアント装置と、VPN ゲートウェイ装置、及び、VPN ゲートウェイ装置に管理されるローカルエリアネットワークに接続された任意の通信装置との間のトンネリングプロトコルによるリモートアクセスVPN を実行するシステムにおいて、

IPネットワーク上に設置されて、リモートアクセスVPNの確立を仲介する仲介装置であって

前記VPNゲートウェイ装置から送信される前記通信装置に割り当てられたプライベートIPアドレスを示す情報（以下、アクセスコントロールリスト）を記憶する手段と、

前記VPNクライアント装置、前記ゲートウェイ装置を認証し、アクセス権限制御を実行する手段と、

前記アクセスコントロールリストを参照して、前記通信装置に割り当てられたプライベートIPアドレスを取得する手段と、

ドメインネームサーバを検索して前記VPNゲートウェイ装置に割り当てられたIPアドレスを取得する手段と、

前記VPNクライアント装置と前記VPNゲートウェイ装置との間の認証に用いる共通鍵を生成する手段と、

前記VPNクライアント装置に、前記VPNゲートウェイ装置のIPアドレス、前記通信装置のプライベートIPアドレス及び共通鍵を送信する手段と、

前記VPNゲートウェイ装置に、前記VPNクライアント装置のIPアドレス及び共通鍵を送信する手段と、

を有することを特徴とする仲介装置。

【請求項 7】

仲介装置とVPNクライアント装置との間の通信、仲介装置とVPNゲートウェイ装置との間の通信を、それぞれ暗号化する手段を有することを特徴とする請求項 6 記載の仲介装置。

【請求項 8】

前記VPNクライアント装置を認証し、認証に成功した場合に限り、前記VPNゲートウェイ装置に割り当てられたIPアドレスをドメインネームサーバに問い合わせ取得し、共通鍵を生成し、取得したIPアドレスと、前記通信装置に割り当てられたプライベートIPアドレス、及び、生成した共通鍵を前記VPNクライアント装置に送信することを特徴とする請求項 6 記載の仲介装置。

【請求項 9】

前記VPNクライアント装置が前記VPNゲートウェイ装置に割り当てられたIPアドレスを検索する権限を有しているか否かを判定し、権限を有している場合に限り、前記VPNゲートウェイ装置に割り当てられたIPアドレスをドメインネームサーバに問い合わせ取得し、共通鍵を生成し、取得したIPアドレス、前記通信装置に割り当てられたプライベートIPアドレス、及び、生成した共通鍵を前記VPNクライアント装置に送信することを特徴とする請求項 6 記載の仲介装置。

【請求項 10】

前記VPNゲートウェイ装置を認証し、認証に成功した場合に限り、前記VPNクライアント装置に割り当てられたIPアドレス、及び、前記共通鍵を前記VPNゲートウェイ装置に送信することを特徴とする請求項 6 記載の仲介装置。

【請求項 11】

SPKI (Simple Public Key Infrastructure) 方式に従って、前記VPNクライアント装置、及び、前記VPNゲートウェイ装置を認証し、及び／または、アクセス権限制御を実行することを特徴とする請求項 6 乃至 10 のいずれか 1 項に記載の仲介装置。

【請求項 12】

PKI (Public Key Infrastructure) 方式に従って、前記VPNクライアント装置、及び、前記VPNゲートウェイ装置を認証することを特徴とする請求項 6 乃至 10 のいずれか 1 項に記載の仲介装置。

【書類名】 明細書

【発明の名称】 リモートアクセスVPN仲介方法及び仲介装置

【技術分野】

【0001】

本発明は、インターネットにおいて、Ipsec (Ip Security Protocol)、L2TP (Layers2 Tunneling Protocol) 等の任意のトンネリングプロトコルによるリモートアクセスVPNを実行するために用いられる情報のうち、VPNクライアント装置のグローバルIPアドレス、VPNゲートウェイ装置のグローバルIPアドレス、VPNクライアント装置とVPNゲートウェイ装置の間で認証に用いる共通鍵等を、VPNクライアント装置とVPNゲートウェイ装置の間で安全に共有する技術に関する。

【背景技術】

【0002】

インターネット上に構築される仮想の閉域ネットワークは一般にバーチャル プライベート ネットワーク (Virtual Private Network: 以後VPNと略す) と呼ばれる。VPNはIPsec、L2TP等のトンネリングプロトコルを用いて構築され、ローカルエリアネットワーク (LAN) 内のリソースに移動クライアントからインターネット経由でアクセスしたり、または、物理的に離れた複数のローカルエリアネットワークをインターネット経由で接続する場合に利用される。

【0003】

トンネリングプロトコルによるリモートアクセスVPNを実現するためには、VPNクライアント装置は、接続先のLANを管理するVPNゲートウェイ装置に割り当てられたグローバルIPアドレスと、接続先であるLAN内の通信装置に割り当てられたプライベートIPアドレスを知る必要がある。また、通信相手を認証し、通信路を暗号化するためには、共通鍵などの鍵情報をVPNクライアント装置とVPNゲートウェイ装置との間で交換することが必要である。

【0004】

リモートアクセスVPNにおけるローカルエリアネットワーク内の通信装置に対するプライベートIPアドレスの割り当て方法としては、(1) VPNゲートウェイ装置のグローバルIPアドレスと同一のIPアドレスをに割り当てる方法、(2) VPNクライアント装置において、プライベートIPアドレスを静的に割り当てる方法、(3) VPNゲートウェイ装置において、DHCP (Dynamic Host Configuration Protocol)、IPCP (PPP IP cotrol Protocol) を用いてアドレスプールから動的に割り当てる方法がある。

【0005】

上記(1)から(3)に示す方法のうち、(1)及び(2)については、VPNクライアント装置は接続先ホストのプライベートIPアドレスを知る必要がない。しかし、(1)については、ローカルエリアネットワークを構成できないという課題がある。また、(2)については、VPNクライアント装置において任意に接続先のプライベートIPアドレスを指定できるため、VPNゲートウェイ装置においてセキュリティポリシーに基づいてローカルエリアネットワークを運用できないという課題がある。また、(3)については、VPNゲートウェイ装置においてプライベートIPアドレスを動的に割り当てるため、VPNクライアント装置は接続先の通信装置に割り当てられたプライベートIPアドレスを知ることができない。

【0006】

一方、DHCPによってVPNクライアント装置にプライベートIPアドレスを動的に割り当てる方法がある (例えば、非特許文献1参照)。ここでは、VPNクライアント装置は接続先のローカルエリアネットワーク内のプライベートIPアドレスを取得してトンネリングプロトコルで接続することにより、VPNクライアント装置はローカルエリアネットワーク上の仮想的なホストとして動作する。しかしながら、ここに示される方法は、クライアント装置にIPアドレスを割り当てるものであり、クライアント装置が有る接続先のIPアドレスを知るためには別の手段を用いる必要がある。

【0007】

また、共通鍵を安全に配布する方法としては種々の方法がある（例えば、特許文献1、特許文献2参照）。特許文献1に示される方法は、ローカルエリアネットワークに接続された複数の通信装置との間で共通鍵を交換する方法で、DHCPサーバ機能を有するゲートウェイ装置を介して共通鍵を交換する。具体的には、ローカルエリアネットワークへの接続時にDHCPに従いIPアドレスを取得する際に、共通鍵も同時に交換する。これによって、ローカルエリアネットワーク内の通信を暗号化するための共通鍵を交換できる。また、特許文献2に示される方法は、インターネットに接続されたVPNクライアント装置と、VPNゲートウェイ装置で管理されるローカルエリアに接続された通信装置との通信において、VPNクライアント装置とVPNゲートウェイ装置との間である共通鍵を交換し、VPNゲートウェイ装置と通信装置との間で別の共通鍵を交換する方法である。これによって、VPNクライアント装置とローカルエリアネットワークに接続された通信装置との間でIKE等の鍵交換方式を用いて鍵交換を行う必要なく、VPNクライアント装置とローカルエリアネットワークに接続された通信装置との暗号通信を実現できる。ここに示される方法は、いずれもゲートウェイ装置を介して共通鍵を安全に配布できるが、プライベートIPアドレスを配布する方法については考慮されていない。

**【0008】**

また、設定情報を管理する管理装置を設け、管理装置が通信装置に設定情報を転送する際に、通信装置のIPアドレスとログインパスワードを提示してその通信装置にログインし、設定情報を転送する方法がある（例えば、特許文献3参照）。これによれば、ゲートウェイ装置に相当する管理装置から設定情報としてプライベートIPアドレスを配布できるが、IPアドレスとログインパスワードの組み合わせによる認証方法で通信端末の偽装を防ぐことは困難である。それは、IPアドレスは偽装可能であり、パスワードは持ち主を特定できないためである。

**【0009】**

また、公開鍵を用いた認証方法、証明書発行方法としてSPKI (Simple Public Key Infrastructure) 方式がある（例えば、非特許文献2、非特許文献3）が、リモートアクセスVPNへの利用方法について明らかでない。

**【0010】**

【特許文献1】特開2001-292135号

【特許文献2】特開2002-271309号公報

【特許文献3】特開 2003-18163号公報

【非特許文献1】B.Patel, B.Aboba, S.Kelly, V.Gupta, 「ダイナミックホスト コンフィグレーション プロトコル (ディーエイチシーピーイ4) コンフィグレーション オブ アイピーセック トンネルモード (Dynamic Host Configuration Protocol (DHCPv4) Configuration of IPsec Tunnel Mode)」, [online]、2003年1月掲載、RFC3456、Internet Engineering Task Force、[2003年3月17日検索]、インターネット<URL: <http://www.ietf.org/rfc/rfc3456.txt>>

【非特許文献2】C.Ellison, B.Frantz, B.Lampson, R.Rivest, B.Thomas, T.Ylonen, 「エスピーケーアイ サーティフィケート セオリー (SPKI Certificate Theory)」, [online]、1999年9月掲載、RFC2693、Internet Engineering Task Force、インターネット<URL: <http://www.ietf.org/rfc/rfc2693.txt>>

【非特許文献3】C.Ellison, B.Frantz, B.Lampson, R.Rivest, B.Thomas, T.Ylonen, 「シンプル パブリック キー インフラストラクチャ <ドラフトーアイイーティーエフエスピーケーアイサートーストラクチャー06.txt> (Simple Public Key Infrastructure <draft-ietf-spki-cert-structure-06.txt>)」, [online]、1999年7月26日掲載、Internet Engineering Task Force、インターネット<URL: <http://world.std.com/~cme/spki.txt>>

【発明の開示】

【発明が解決しようとする課題】

**【0011】**

本発明は、上述のような課題に鑑みなされたものであり、IPネットワークにおいて、IPsec、L2TP等の任意のトンネリングプロトコルによるリモートアクセスVPNを実行するために用いる情報のうち、VPNクライアント装置のグローバルIPアドレス、VPNゲートウェイ装置のグローバルIPアドレス、VPNゲートウェイ装置により管理されるローカルエリアネットワーク内の任意の通信装置のプライベートIPアドレス、及び、VPNクライアント装置とVPNゲートウェイ装置の間でIKEフェーズ1における認証に用いる共通鍵を、VPNクライアント装置とVPNゲートウェイ装置との間で安全に共有できるようにすることである。また、リモートアクセスVPNにおける認証において、利用者の個人情報を通信する相手に知られずに通信できるようにすることである。

【課題を解決するための手段】

【0012】

本発明は、IPネットワークに、リモートアクセスVPNの動作を仲介する仲介装置を設けたことを主要な特徴とする。

【0013】

仲介装置は、IPネットワークに接続したVPNクライアント装置、及び、VPNゲートウェイ装置と、VPNゲートウェイ装置により管理されるローカルエリアネットワークに接続した任意の通信装置との間のIPsec、L2TP等の任意のトンネリングプロトコルによるリモートアクセスVPNを確立するために用いる情報（コントロールアクセスリスト）を記憶する。この情報には、通信装置に割り当てられたプライベートIPアドレスが含まれる。

【0014】

仲介装置は、VPNクライアント装置からVPNゲートウェイ装置に割り当てられたIPアドレスの検索要求を受信したら、VPNクライアント装置がVPNゲートウェイ装置に割り当てられたIPアドレスを検索する権限を有するかどうかを検証する。そして、権限を有する場合に限り、アクセスコントロールリストを参照して、VPNゲートウェイ装置により管理されるローカルエリアネットワークに接続した通信装置に割り当てられたプライベートIPアドレスを取得し、ドメインネームサーバ（DNS）を検索してVPNゲートウェイ装置に割り当てられたIPアドレスを取得し、VPNクライアント装置とVPNゲートウェイ装置との間のIKE等の認証に用いる共通鍵を生成する。次に、仲介装置とVPNクライアント装置との間の通信路を暗号化して、VPNゲートウェイ装置に割り当てられたIPアドレス、通信装置に割り当てられたプライベートIPアドレス及び生成した共通鍵をVPNクライアント装置に送信する。また、仲介装置とVPNゲートウェイ装置との通信路を暗号化して、VPNクライアント装置に割り当てられたIPアドレス及び生成した共通鍵をVPNゲートウェイ装置に送信する。

【0015】

また、仲介装置は、SPKI方式に従って、VPNクライアント装置、及び、VPNゲートウェイ装置を認証する。また、VPNクライアント装置は、SPKI方式に従って証明書を発行する。さらに、仲介装置はPKI方式に従って、VPNクライアント装置、及び、VPNゲートウェイ装置を認証することも可能とする。

【0016】

また、仲介装置は、公開鍵、FQDN（Fully Qualified Distinguished Name）、GUID（Globally Unique Identifier）、MACアドレス、SPKI（Simple Public Key Infrastructure）Local Name、X.500 Distinguish Name等の任意の名前形式に従ってVPNクライアント装置、VPNゲートウェイ装置、及び、通信装置を識別することも可能とする。これによって、IPsec、L2TPなどの任意のトンネリングプロトコル、PKI、SPKI、パスワードなどの任意の認証方式を組み合わせるリモートアクセスVPNを実行できる。

【発明の効果】

【0017】

本発明においては、次のような効果を奏する。第1の効果は、IPネットワークにおいて、L2TP、IPsec等のトンネリングプロトコルによるリモートアクセスVPNを実行するために用いる情報のうち、VPNクライアント装置のグローバルIPアドレス、VPNゲートウェイ装置のグローバルIPアドレス、VPNゲートウェイ装置により管理されるローカルエリアネット



ワーク内の任意の通信装置のプライベートIPアドレス、及び、VPNクライアント装置とVPNゲートウェイ装置の間でIKEフェーズ1における認証に用いる共通鍵を、VPNクライアント装置とVPNゲートウェイ装置との間で安全に共有できることである。その理由は、仲介装置においてプライベートIPアドレスを安全に管理し、プライベートIPアドレスと共通鍵を安全に配布するためである。

【0018】

具体的には、プライベートIPアドレスの仲介装置への登録において、VPNゲートウェイ装置を認証し、認証に成功した場合に限り、通信路を暗号化し、暗号化した通信路を用いて、プライベートIPアドレスを受信する。また、プライベートIPアドレスの検索において、VPNクライアント装置を認証し、認証に成功した場合に限り、VPNクライアント装置の公開鍵を用いてアクセス権限制御を実行し、アクセス権限制御に成功した場合に限り、VPNゲートウェイ装置のグローバルIPアドレスをドメインネームサーバDNSに提示して検索し、仲介装置とVPNクライアント装置との間の通信路を暗号化し、暗号化した通信路を用いて、VPNゲートウェイ装置のグローバルIPアドレスと、通信装置のプライベートIPアドレスと、共通鍵をVPNクライアント装置に送信し、また、仲介装置とVPNゲートウェイ装置との通信路を暗号化し、暗号化した通信路を用いて、VPNクライアント装置のグローバルIPアドレスと、共通鍵をVPNゲートウェイ装置に送信するためである。

【0019】

第2の効果は、リモートアクセスVPNにおける認証において、利用者の個人情報を通信する相手に知られずに通信できる手段を提供することである。その理由は、PKI方式に従って認証する場合には、個人情報を含む公開鍵証明書を通信相手に送信する代わりに仲介装置に送信して認証するためである。また、SPKI方式に従って認証する場合には、いかなる証明書も個人情報を含まないように証明書の形式を定義できるためである。

【発明を実施するための最良の形態】

【0020】

以下に、本発明の実施の形態について図面を参照して詳細に説明する。

【実施例1】

【0021】

これは、SPKI (Simple Public Infrastructure) 方式に従って、仲介装置がVPNクライアント装置やVPNゲートウェイ装置を認証し、また、VPNクライアント装置が権限委譲の証明書を発行する実施例である。このSPKI方式では認証局は不要である。

【0022】

図1に本実施例の全体的システム構成を示す。図1において、VPNクライアント装置 (A) 101、VPNクライアント装置 (D) 102、VPNゲートウェイ装置 (B) 103、仲介装置 (S) 104、ドメインネームサーバ (DNS) 105はそれぞれIP (Internet Protocol) に従ってネットワーク (WAN) 100に接続されている。また、通信装置 (C) 111が、VPNゲートウェイ装置 (B) 103をゲートウェイ装置とするローカルエリアネットワーク (LAN) 110に接続されている。

【0023】

図2は、図1の全体の動作を説明するための図である。太線はIpsecトンネルモードによるVPNを示している。

【0024】

ここで、VPNクライアント装置 (A) 101のホスト名は公開鍵PUBLICKEY\_A (またはそのハッシュ値HASH\_A)、IPアドレスはIPADDRESS\_Aとする。VPNクライアント装置 (D) 102のホスト名は公開鍵PUBLICKEY\_D (またはそのハッシュ値HASH\_D)、IPアドレスはIPADDRESS\_Dとする。また、VPNゲートウェイ装置 (B) 103のホスト名は公開鍵PUBLICKEY\_B (またはそのハッシュ値HASH\_B、IPアドレスはIPADDRESS\_B) とする。すなわち、VPNクライアント装置やVPNゲートウェイ装置は、それぞれ、その公開鍵 (またはそのハッシュ値) で識別可能である。通信装置 (C) 111のプライベートIPアドレスはIPADDRESS\_Cとする。

## 【0025】

VPNクライアント装置 (A) 101に割り当てられたIPアドレスIPADDRESS\_A、VPNゲートウェイ装置 (B) 103に割り当てられたIPアドレスIPADDRESS\_B、及び、VPNクライアント装置 (D) 102に割り当てられたIPアドレスIPADDRESS\_DはいずれもIPネットワーク (WAN) 100において一意であり、任意の手段で動的に割り当てられる。VPNゲートウェイ装置 (B) 103の公開鍵PUBLICKEY\_BとIPアドレスIPADDRESS\_Bはドメインネームサーバ (DNS) 105において一意に関連付けられて管理される。また、通信装置 (C) 111に割り当てられたプライベートIPアドレスIPADDRESS\_Cはローカルエリアネットワーク (LAN) 110において一意であり、任意の手段を用いて動的に割り当てられる。

## 【0026】

VPNクライアント装置 (A) 101、VPNクライアント装置 (D) 102、VPNゲートウェイ装置 (B) 103、及び、仲介装置 (S) 104は、IPsecトランスポートモード、または、IPsecトンネルモードにより通信路を暗号化する手段を有する。また、VPNクライアント装置 (A) 101は、公開鍵PUBLICKEY\_Aと対の秘密鍵PRIVATEKEY\_Aを、PUBLICKEY\_Aとともに保管している。VPNゲートウェイ装置 (B) 103は、公開鍵PUBLICKEY\_Bと対の秘密鍵PRIVATEKEY\_Bを、PUBLICKEY\_Bとともに保管している。VPNクライアント装置 (D) 102は、公開鍵PRIVATEKEY\_Dと対の秘密鍵PRIVATEKEY\_BをPUBLICKEY\_Dとともに保管している。VPNゲートウェイ装置 (B) 103は、アクセスコントロールリスト (ACL) を保管している。図6に本実施例におけるアクセスコントロールリスト (ACL) の例を示す。アクセスコントロールリスト (ACL) の文法はSPKI (Simple Public Key Infrastructure) に関する先の非特許文献2、及び非特許文献3で定義されている。

## 【0027】

仲介装置 (S) 104は、(1) VPNゲートウェイ装置 (B) 103の公開鍵PUBLICKEY\_Bをドメインネームサーバ (DNS) 105に提示して、VPNゲートウェイ装置 (B) 103に割り当てられたIPアドレスIPADDRESS\_Bを取得する手段、(2) VPNゲートウェイ装置 (B) 103で保管されるアクセスコントロールリスト (ACL) を記憶する手段、(3) SPKI方式に基づいて、VPNクライアント装置 (A) 101、VPNゲートウェイ装置 (B) 103を認証し、及び／または、アクセス権限制御を実行する手段、(4) 後述の共通鍵KEY\_AB、及び、KEY\_DBを生成する手段を具備している。

## 【0028】

上記(1)の手段では、DNS方式と呼ばれるインターネットにおける一般的な名前解決方式に従って、公開鍵PUBLICKEY\_BからIPアドレスIPADDRESS\_Bを解決する。また、上記(2)の手段では、公開鍵PUBLICKEY\_Bとアクセスコントロールリスト (ACL) を関連付けて管理する。

## 【0029】

また、上記(3)の手段では、SPKI方式に従い、VPNクライアント装置 (A)、VPNゲートウェイ装置 (B) 103、及び、VPNクライアント装置 (D) 102を認証する。具体的には、秘密鍵PRIVATEKEY\_Aによる署名SIG\_Aと公開鍵PUBLICKEY\_Aをすべて入力して、署名SIG\_Aを確認することにより、秘密鍵PRIVATEKEY\_Aの本人性を証明する。同様に、秘密鍵PRIVATEKEY\_Bによる署名SIG\_Bと公開鍵PUBLICKEY\_Bをすべて入力して、署名SIG\_Bを確認することにより、秘密鍵PRIVATEKEY\_Bの本人性を証明する。同様に、秘密鍵PRIVATEKEY\_Dによる署名SIG\_D、及び、公開鍵PUBLICKEY\_Dをすべて入力して、署名SIG\_Dを確認することにより、秘密鍵PRIVATEKEY\_Dの本人性を証明する。また、上記(3)の手段では、SPKI方式に従い、VPNゲートウェイ装置 (B) 103に対するVPNクライアント装置 (A) 101、及び、VPNクライアント装置 (D) 102のアクセス権限を制御する。VPNゲートウェイ装置 (B) 103に対するVPNクライアント装置 (A) 101のアクセス権限を制御する場合には、VPNゲートウェイ装置 (B) 103のIPアドレスIPADDRESS\_Bを検索するためのDNSクエリQUERY、署名SIG\_A、及び、アクセスコントロールリスト (ACL) を入力して、SPKIに関する非特許文献2、及び、非特許文献3において定義される5-tuple reduction演算規則、及び／または、4-tuple reduction演算規則に基づく演算を実行して、演算結果を出力

する。また、VPNゲートウェイ装置 (B) 103 に対するVPNクライアント装置 (D) 102 のアクセス権限を制御する場合には、VPNゲートウェイ装置 (B) 103 のIPアドレスIPADDRESS\_Bを検索するためのDNSクエリQUERY、署名SIG\_D、SPKIに関する非特許文献2及び非特許文献3において定義される証明書CERT、及び、アクセスコントロールリスト (ACL) を入力して、SPKIに関する非特許文献2、及び、非特許文献3において定義される5-tuple reduction演算規則、及び/または、4-tuple reduction演算規則に基づく演算を実行して、演算結果を出力する。演算結果の具体例については、図8を参照して後述する。

#### 【0030】

また、上記(4)の手段は、VPNクライアント装置 (A) 101とVPNゲートウェイ装置 (B) 103との間のIKEフェーズ1における認証に用いる共通鍵KEY\_AB、または、VPNクライアント装置 (D) 102とVPNゲートウェイ装置 (B) 103との間のIKEフェーズ1における認証に用いるKEY\_DBをそれぞれ生成する。

#### 【0031】

また、VPNクライアント装置 (A) 101は、SPKI方式に従って、VPNクライアント装置 (D) 102に対し言言委譲の証明書CERTを発行する機能を有する。SPKIに関する非特許文献2及び非特許文献3においては、権限証明書 (Authorization Certificate) と名前証明書 (Name Certificate) の2種類の証明書について、それぞれ文法を定義している。本実施例においては、説明を簡単にするために、証明書CERTは権限証明書の1種類であると定義する。図9に本実施例における証明書CERTの具体例を示す。SPKIに関する非特許文献2及び非特許文献3によれば、権限証明書は、発行者の秘密鍵と一意に対応した公開鍵またはその公開鍵のハッシュ値を定義するissuerフィールド、権限の行使者の秘密鍵と一意に対応した公開鍵またはその公開鍵のハッシュ値を定義するsubjectフィールド、権限内容を定義した文字列を含むtagフィールド、権限委譲を許可するか否かを定義した文字列を含むdelegationフィールド、及び、権限証明書の有効期間を定義した文字列を含むvalidityフィールドから構成されるデータ (以後、本データを証明書情報INFOと呼ぶ) に対し、発行者の秘密鍵で署名したデータである。この定義に基づき、本実施例における証明書CERTの証明書情報INFOにおけるissuerフィールドの値は、公開鍵PUBLICKEY\_Aまたは任意のハッシュ演算アルゴリズムによる公開鍵PUBLICKEY\_Aのハッシュ値HASH\_Aであると定義する。かつ、subjectフィールドの値は、公開鍵PUBLICKEY\_Dまたは任意のハッシュ演算アルゴリズムによる公開鍵PUBLICKEY\_Dのハッシュ値HASH\_Dであると定義する。かつ、tagフィールドの値は、VPNゲートウェイ装置 (B) 103のIPアドレスIPADDRESS\_Bであると定義する。かつ、delegationフィールドの値は、非特許文献2において定義される文字列「(propagate)」であると定義する。一方、validityフィールドの値は、本発明とは直接関係しないため、いかなる値も定義しないものとする。また、証明書情報INFOに秘密鍵PRIVATEKEY\_Aを用いて署名する。

#### 【0032】

次に、図2を参照して、図1の動作概要を説明する。アクセスコントロール (ACL) の登録 (記憶) 時、VPNゲートウェイ装置 (B) 103は、公開鍵PUBLICKEY\_B (またはそのHASH\_B) とアクセスコントロール (ACL) を仲介装置 (S) 104に送信する (ステップ1)。仲介装置 (S) 104は該公開鍵PUBLICKEY\_B (またはそのHASH\_B) とアクセスコントロール (ACL) を記憶する。

#### 【0033】

VPNゲートウェイ装置 (B) 103を経由して、VPNクライアント装置 (A) 101から通信装置 (C) 111にIpsecトンネルモードによるリモートVPNを実行する場合、VPNクライアント装置 (A) 101は、公開鍵PUBLICKEY\_Aと公開鍵PUBLICKEY\_B (またはそのHASH\_B) (を仲介装置 (S) 104に送信して、VPNゲートウェイ装置 (B) 103及び通信装置 (C) IPアドレスの検索要求を行なう (ステップ2)。

#### 【0034】

仲介装置 (S) 104は、SPKI方式に従ってVPNクライアント装置 (A) 101のアクセス権限制御を実行し、アクセスを許可する場合には、ドメインネームサーバ (DNS) 10

5を検索してVPNゲートウェイ装置(B)103に割り当てられたIPアドレスIPADDRESS\_Bを取得する(ステップ3)。また、仲介(S)104は、アクセスコントロール(ACL)を参照して、VPNゲートウェイ装置(B)103により管理されるLAN110に接続された通信装置(C)111に割り当てられたプライベートIPアドレスIPADDRESS\_Cを取得する。さらに、仲介装置(S)104は、VPNクライアント装置(A)101との間の認証に用いる共通鍵KEY\_ABを生成する。そして、仲介装置(S)104は、仲介装置(S)104とVPNクライアント装置(A)101との間の通信路を暗号化し、VPNクライアント装置(A)101へIPADDRESS\_B、IPADDRESS\_C及び共通鍵KEY\_ABを送信する(ステップ4)。また、仲介装置(S)104は、仲介装置(S)104とVPNゲートウェイ装置(B)103との間の通信路を暗号化し、VPNゲートウェイ装置(B)103へIPADDRESS\_AとKEY\_ABを送信する(ステップ5)。

#### 【0035】

また、VPNクライアント装置(A)101は、VPNゲートウェイ装置(B)103のIPアドレスを検索する権限をVPNクライアント装置(D)102委譲する場合、VPNクライアント装置(D)102に対してSPKI方式に従って証明書CERTを送信する(ステップ6)。VPNクライアント装置(D)102は、公開鍵PUBLICKEY\_DとCERT、及び公開鍵PUBLICKEY\_B(またはそのHASH\_B)仲介装置(S)104に送信して、VPNゲートウェイ装置(B)103及び通信装置(C)のIPアドレスの検索要求を行なう(ステップ7)。

#### 【0036】

仲介装置(S)104は、SPKI方式に従ってVPNクライアント装置(D)102のアクセス権限制御を実行し、アクセスを許可する場合には、ドメインネームサーバ(DNS)105を検索してVPNゲートウェイ装置(B)103に割り当てられたIPアドレスIPADDRESS\_Bを取得する(ステップ8)。また、仲介装置(S)104は、アクセスコントロール(ACL)を参照して、VPNゲートウェイ装置(B)103により管理されるLAN110に接続された通信装置(C)111に割り当てられたプライベートIPアドレスIPADDRESS\_Cを取得する。さらに、仲介装置(S)104は、VPNクライアント装置(D)102との間の認証に用いる共通鍵KEY\_DBを生成する。そして、仲介装置(S)104は、仲介装置(S)104とVPNクライアント装置(D)102との間の通信路を暗号化し、VPNクライアント装置(d)102へIPADDRESS\_B、IPADDRESS\_C及び共通鍵KEY\_DBを送信する(ステップ9)。また、仲介装置(S)104は、仲介装置(S)104とVPNゲートウェイ装置(B)103との間の通信路を暗号化し、VPNゲートウェイ装置(B)103へIPADDRESS\_DとKEY\_DBを送信する(ステップ10)。

#### 【0037】

以上、図1に示すシステムの各装置の構成及び全体の動作概要を述べたが、ドメインネームサーバ(DNS)105におけるIPアドレスの管理及び名前解決方法、IPsecトランスポートモードまたはトンネルモードによる通信路の暗号化方法、共通鍵KEY\_AB及びKEY\_DBの生成方法、及び、公開鍵を用いた署名確認方法については、当業者にとってよく知られているので、その詳細な構成は省略する。また、SPKI方式におけるアクセス権限制御において、権限証明書に加え、名前証明書を用いる場合も本実施例と同様の方法で実施できるため、その詳細な説明については省略する。

#### 【0038】

以下に、本実施例1におけるアクセスコントロールリスト(ACC)の記憶手順、及びIPアドレスの取得共通鍵の生成、これらIPアドレスと共通鍵の送信手順について詳述する。

#### 【0039】

まず、図3を参照して、VPNゲートウェイ装置(B)103において保管されるアクセスコントロールリスト(ACL)を仲介装置(S)104に記憶する手順について説明する。

VPNゲートウェイ装置(B)103と仲介装置(S)104は、IPsecトランスポートモードにより接続する(ステップ1001)。これでVPNゲートウェイ装置(B)103と仲介装置(S)104との間の通信路が暗号化される。VPNゲートウェイ装置(B)103は、暗号化された通信路を用いて、公開鍵PUBLICKEY\_BとSKPI形式のアクセスコントロールリ

スト (ACL) (図6) をすべて送信する (ステップ1002)。仲介装置 (S) 104は、VPNゲートウェイ装置 (B) 103から送信された公開鍵PUBLICKEY\_Bとアクセスコントロールリスト (ACL) を受信して、該受信した公開鍵PUBLICKEY\_Bとアクセスコントロールリスト (ACL) を関連づけて記憶する (ステップ1003)。VPNゲートウェイ装置 (B) 103と仲介装置 (S) 104は、接続を切断する (ステップ1004)。

次に、図4及び図5を参照して、仲介装置 (S) 104が、VPNクライアント装置 (A) 101とVPNゲートウェイ装置 (B) 103との間の共通鍵KEY\_ABを生成し、VPNゲートウェイ装置 (B) 103に割り当てられたIPアドレスIPADDRESS\_B、通信装置 (C) に割り当てられたプライベートIPアドレスIPADDRESS\_C、及び、共通鍵KEY\_ABをVPNクライアント装置 (A) 101に送信し、また、VPNクライアント装置 (A) 101に割り当てられたIPアドレスIPADDRESS\_A、及び、共通鍵KEY\_ABをVPNゲートウェイ装置 (B) 103に送信する手順について説明する。

#### 【0040】

図4において、VPNクライアント装置 (A) 101と仲介装置 (S) 104は、IPsecトランスポートモードにより接続する (ステップ1101)。すなわち、VPNクライアント装置 (A) 101と仲介装置 (S) 104との間の通信路が暗号化される。VPNクライアント装置 (A) 101は、暗号化された通信路を用いて、VPNゲートウェイ装置 (B) 103の公開鍵PUBLICKEY\_Bを含むDNSクエリQUERY、及び、VPNクライアント装置 (A) 101の公開鍵PUBLICKEY\_Aをすべて送信する (ステップ1102)。

#### 【0041】

仲介装置 (S) 104は、VPNクライアント装置 (A) 101に割り当てられたIPアドレスIPADDRESS\_A、VPNゲートウェイ装置 (B) 103に割り当てられたIPアドレスIPADDRESS\_B、VPNゲートウェイ装置 (B) 103により管理されるLAN110に接続される通信装置 (C) 111に割り当てられたプライベートIPアドレスIPADDRESS\_Cを取得し、VPNクライアント装置 (A) 101とVPNゲートウェイ装置 (B) 103との間のIKE等の認証に用いる共通鍵KEY\_ABを生成する (ステップ1103)。図5はステップ1103の詳細処理フローである。

#### 【0042】

図5において、仲介装置 (S) 104は、VPNクライアント装置 (A) 101から送信されたDNSクエリQUERYと公開鍵PUBLICKEY\_Aをすべて受信して入力する (ステップ1201)。次に、入力したDNSクエリQUERYを参照して、公開鍵PUBLICKEY\_Bをすべて取得する (ステップ1202)。次に、取得した公開鍵PUBLICKEY\_Bをもとに、関連付けられたアクセスコントロールリスト (ACL) をすべて取得する (ステップ1203)。アクセスコントロールリスト (ACL) は図6に示す形式をとる。次に、ステップ1201において入力したDNSクエリQUERYを用いて、図7に示す形式のデータTAGを生成する (ステップ1204)。

#### 【0043】

仲介装置 (S) 104は、上記ステップ1201において入力した公開鍵PUBLICKEY\_Aとステップ1204において生成したデータTAGとステップ1203において取得したアクセスコントロールリスト (ACL) をすべて入力し、例えば、非特許文献2、及び、非特許文献3において定義される演算規則に従って演算を実行し (ステップ1205)、演算に成功する否か判定する (ステップ1206)。演算に失敗した場合、この時点で処理を終了とする。

#### 【0044】

仲介装置 (S) 104は、ステップ1206において、演算に成功した場合と判定された場合に限り、図8に示す形式の演算結果のデータDATAを出力する。図8に示す演算結果データDATAは非特許文献2、及び、非特許文献3で定義される5-tuple形式のデータである。演算結果データDATAのsubjectフィールドの値がステップ1201において受信した公開鍵PUBLICKEY\_AのSHA-1アルゴリズムによるハッシュ値HASH\_Aと完全一致しているACLエントリが、ステップ1203において取得したアクセスコントロールリスト (ACL) に含

まれる場合に限り、データDATAのtagフィールドにはデータTAGと完全一致する文字列が含まれる。

#### 【0045】

仲介装置 (S) 104 は、出力されたデータDATAのtagフィールドを参照して、DNSクエリQUERY' を生成する (ステップ1207)。次に、DNSクエリQUERY' をドメインネームサーバ (DNS) 105 に提示して検索し、IPアドレスIPADDRESS\_Bを取得する (ステップ1208)。次に、公開鍵PUBLICKEY\_Aのハッシュ値HASH\_AをもとにアクセスコントロールリストACLを検索し、(subjectフィールドの値にハッシュ値HASH\_Aと完全一致する文字列を含む (ACL) エントリENTRYを取得する (ステップ1209)。次に、ステップ1209において取得したACLエントリENTRYのtagフィールドを参照して、プライベートIPアドレスIPADDRESS\_Cを取得する (ステップ1210)。次に、VPNクライアント装置 (A) 101 のIPアドレスIPADDRESS\_Aを取得する (ステップ1211)。次に、共通鍵KEY\_ABを生成する (ステップ1212)。

#### 【0046】

図4に戻り、仲介装置 (S) 104 は、ステップ1101において暗号化された通信路を用いて、上記取得したIPアドレスIPADDRESS\_B、取得したプライベートIPアドレスIPADDRESS\_C、及び、生成した共通鍵KEY\_ABをすべてVPNクライアント装置 (A) 101 に送信する (ステップ1104)。次に、クライアント装置 (A) 101 と仲介装置 (S) 104 は、接続を切断する (ステップ1105)。

#### 【0047】

次に、VPNゲートウェイ装置 (B) 103 と仲介装置 (S) 104 は、IPsecトランスポートモードにより接続する (ステップ1106)。すなわち、VPNゲートウェイ装置 (B) 103 と仲介装置 (S) 104 との間の通信路が暗号化される。次に、仲介装置 (S) 104 は、ステップ1106において暗号化された通信路を用いて、先に取得したIPアドレスIPADDRESS\_A、及び、先にて生成した共通鍵KEY\_ABをすべてVPNゲートウェイ装置 (B) 103 に送信する (ステップ1107)。次に、VPNゲートウェイ装置 (B) 103 と仲介装置 (S) 104 は、接続を切断する (ステップ1108)。

#### 【0048】

その後、図2に示したようなVPNゲートウェイ装置 (B) 103 を経由して、クライアント装置 (A) 101 から通信装置 (C) 111 にIpsecトンネルモードによるリモートアクセスVPNが実行されるが、その詳細は省略する。

#### 【0049】

次に、VPNクライアント装置 (A) 101 において証明書CERTを発行し、発行した証明書CERTをVPNクライアント装置 (D) 102 に渡す手順を以下に示す。なお、その処理フロー図は省略する。

(1) VPNクライアント装置 (A) 101 は、SPKI方式において定義された文法に従い、証明書CERTの証明書情報INFOを生成する。本実施例における証明書CERTの実施例を図9に示す。図9において、証明書情報INFOにおけるissuerフィールドの値は、公開鍵PUBLICKEY\_Aの任意のハッシュ演算アルゴリズムによるハッシュ値HASH\_Aであると定義する。かつ、subjectフィールドの値は、公開鍵PUBLICKEY\_DのSHA-1アルゴリズムによるハッシュ値HASH\_Dであると定義する。かつ、tagフィールドの値は、VPNゲートウェイ装置Bに割り当てられたIPアドレスIPADDRESS\_Bであると定義する。かつ、delegationフィールドの値は、非特許文献3において定義される文字列「(propagate)」であると定義する。一方、validityフィールドの値は、本発明とは直接関係しないため、任意の値を定義してもよい。

(2) VPNクライアント装置 (A) 101 は、上記 (1) において生成したデータに秘密鍵PRIVATEKEY\_Aを用いて署名することにより、証明書CERTを発行する。

(3) VPNクライアント装置 (A) 101 は、上記 (2) において発行した証明書CERTを任意の手段でVPNクライアント装置 (D) 102 にすべて送信する。

(4) VPNクライアント装置 (D) 102 は、VPNクライアント装置 (A) 101 から送信された証明書CERTを任意の手段ですべて受信し、記憶する。



## 【0050】

仲介装置 (S) 104 が、VPNクライアント装置 (D) 102 とVPNゲートウェイ装置 (B) 103 との間のIKE等の認証に用いる共通鍵KEY\_DBを生成し、次に、IPアドレスIPADDRESS\_B、プライベートIPアドレスIPADDRESS\_C、及び、共通鍵KEY\_DBをVPNクライアント装置 (D) 102 に送信し、次に、VPNクライアント装置 (D) 102 に割り当てられたIPアドレスIPADDRESS\_D、及び、共通鍵KEY\_DBをVPNゲートウェイ装置 (B) 103 に送信する手順は、先の図4及び図5において説明した仲介装置 (S) が、VPNクライアント装置 (A) 101 とVPNゲートウェイ装置 (B) 103 との間の共通鍵KEY\_ABを生成して、IPアドレスIPADDRESS\_B、プライベートIPアドレスIPADDRESS\_C、及び、共通鍵KEY\_ABをVPNクライアント装置 (A) 101 に送信し、また、IPアドレスIPADDRESS\_A、及び、共通鍵KEY\_ABをVPNゲートウェイ装置 (B) 103 に送信する手順と同様の手順で実施できる。

## 【0051】

このようにして、図2に示したように、VPNゲートウェイ装置 (B) 103 を経由して、VPNクライアント装置 (D) 102 から通信装置 (C) 111 にIpsecトンネルモードによるリモートアクセスVPNが実行することが可能になる。

## 【0052】

以上述べたように、本実施例において、仲介装置 (S) 104 は、VPNゲートウェイ装置 (B) 103 より送信されたアクセスコントロールリスト (ACL) を記憶することで、通信装置 (C) 111 に割り当てられたプライベートIPアドレスIPADDRESS\_Cを記憶する。これによって、仲介装置 (S) 104 は、VPNゲートウェイ装置 (B) 103 だけが知っている、ローカルエリアネットワーク (LAN) 110 に接続された通信装置 (C) 111 に割り当てられたプライベートIPアドレスIPADDRESS\_Cを知ることができる。従って、VPNクライアント装置 (A) 101 は、VPNゲートウェイ装置 (B) 103 を介した通信装置 (C) 111 へのIPsecトンネルモードによるリモートアクセスVPNに必要なプライベートIPアドレスIPADDRESS\_Cを、リモートアクセスVPNを実行する前に仲介装置 (S) 104 に問い合わせることにより知ることができる。

## 【0053】

また、本実施例において、仲介装置 (S) 104 は、共通鍵KEY\_ABを生成し、生成した共通鍵KEY\_ABをVPNクライアント装置 (A) 101 とVPNゲートウェイ装置 (B) 103 の両者に送信する。これによって、VPNクライアント装置 (A) 101 とVPNゲートウェイ装置 (B) 103 はともに共通鍵KEY\_ABを受信できる。従って、VPNクライアント装置 (A) 101 とVPNゲートウェイ装置 (B) 103 はIKEフェーズ1における認証に用いる共通鍵KEY\_ABをオンラインで共有できる。

## 【0054】

また、本実施例において、仲介装置 (S) 104 は、VPNゲートウェイ装置 (B) 103 を認証し、認証に成功した場合に限り、VPNゲートウェイ装置 (B) 103 より送信された、通信装置 (C) 111 に割り当てられたプライベートIPアドレスIPADDRESS\_Cを、仲介装置 (S) 104 に記憶する。これによって、仲介装置 (S) 104 は、偽装されていないVPNゲートウェイ装置 (B) 103 から送信されたプライベートIPアドレスIPADDRESS\_Cに限り記憶できる。従って、VPNクライアント装置 (A) 101 は、正しいVPNゲートウェイ装置 (B) 103 から送信されたプライベートIPアドレスIPADDRESS\_Cを知ることができる。

## 【0055】

また、本実施例において、仲介装置 (S) 104 は、VPNゲートウェイ装置 (B) 103 を認証し、認証に成功した場合に限り、VPNゲートウェイ装置 (B) 103 より送信された、通信装置 (C) 111 に割り当てられたプライベートIPアドレスIPADDRESS\_Cを記憶するという動作において、仲介装置 (S) 104 とVPNゲートウェイ装置 (B) 103 との間の通信路を暗号化する。これによって、仲介装置 (S) 104 は、VPNゲートウェイ装置 (B) 103 から送信された、通信装置 (C) 111 に割り当てられたプライベートIPアドレスIPADDRESS\_Cを改ざんされることなく、かつ、盗聴されることなく受信できる。従って、VPNクライアント装置 (A) 101 は、正しいVPNゲートウェイ装置 (B) 103 から送信

された、通信装置 (C) 111 に割り当てられた正しいプライベート IP アドレス IPADDRESS\_C を知ることができる。また、VPN ゲートウェイ装置 (B) 103、通信装置 (C) 111 に割り当てられた正しいプライベート IP アドレス IPADDRESS\_C を不特定多数に知られることなく仲介装置 (S) 104 に送信できる。

【0056】

また、本実施例において、仲介装置 (S) 104 は、VPN クライアント装置 (A) 101 を認証し、認証に成功した場合に限り、VPN ゲートウェイ装置 (B) 103 に割り当てられた IP アドレス IPADDRESS\_B をドメインネームサーバ (DNS) 105 に問い合わせ取得し、共通鍵 KEY\_AB を生成し、取得した IP アドレス IPADDRESS\_B、通信装置 (C) 111 に割り当てられた IP アドレス IPADDRESS\_B、及び、生成した共通鍵 KEY\_AB をすべて VPN クライアント装置 (A) 101 に送信するという動作を実行する。これによって、仲介装置 (S) 104 は、VPN クライアント装置 (A) 101 が偽装されていない場合に限り、VPN ゲートウェイ装置 (B) 103 に割り当てられた IP アドレス IPADDRESS\_B、通信装置 (C) 111 に割り当てられたプライベート IP アドレス IPADDRESS\_C、及び、共通鍵 KEY\_AB のすべてを VPN クライアント装置 (A) 101 に送信できる。従って、正しい VPN クライアント装置 (A) 101 に限り、VPN ゲートウェイ装置 (B) 103 を介して、通信装置 (C) 111 と IPsec トンネルモードによるリモートアクセス VPN を実行できる。

【0057】

また、本実施例において、仲介装置 (S) 104 は、VPN クライアント装置 (A) 101 が VPN ゲートウェイ装置 (B) 103 に割り当てられた IP アドレス IPADDRESS\_B を検索する権限を有しているか否かを判定し、権限を有している場合に限り、VPN ゲートウェイ装置 (B) 103 に割り当てられた IP アドレス IPADDRESS\_B をドメインネームサーバ (DNS) 105 に問い合わせ取得し、共通鍵 KEY\_AB を生成し、取得した IP アドレス IPADDRESS\_B、通信装置 (C) 111 に割り当てられた IP アドレス IPADDRESS\_B、及び、生成した共通鍵 KEY\_AB をすべて VPN クライアント装置 (A) 101 に送信するという動作を実行する。これによって、仲介装置 (S) 104 は、VPN ゲートウェイ装置 (B) 103 に割り当てられた IP アドレス IPADDRESS\_B、通信装置 (C) 111 に割り当てられたプライベート IP アドレス IPADDRESS\_C、及び、共通鍵 KEY\_AB のすべてを、VPN ゲートウェイ装置 (B) 103、及び、通信装置 (C) 111 に対しあらかじめアクセス権限を有する VPN クライアント装置 (A) 101 だけに送信できる。従って、VPN ゲートウェイ装置 (B) 103、及び、通信装置 (C) 111 に対する、不特定多数からの IPsec トンネルモードによるリモートアクセス VPN を防止できる。

【0058】

また、本実施例において、仲介装置 (S) 104 は、仲介装置 (S) 104 と VPN クライアント装置 (A) 101 との間の通信を暗号化する。これによって、仲介装置 (S) 104 は、VPN ゲートウェイ装置 (B) 103 に割り当てられた IP アドレス IPADDRESS\_B、通信装置 (C) 111 に割り当てられたプライベート IP アドレス IPADDRESS\_C、及び、共通鍵 KEY\_AB を改ざんされことなく、かつ、盗聴されことなく VPN クライアント装置 (A) 101 に送信できる。従って、VPN クライアント装置 (A) 101 は、正しい VPN ゲートウェイ装置 (B) 103 を介して、正しい通信装置 (C) 111 と、IPsec トンネルモードによるリモートアクセス VPN を実行できる。

【0059】

また、本実施例において、仲介装置 (S) 104 は、VPN ゲートウェイ装置 (B) 103 を認証し、認証に成功した場合に限り、VPN クライアント装置 (A) 101 に割り当てられた IP アドレス IPADDRESS\_A、及び、共通鍵 KEY\_AB を VPN ゲートウェイ装置 (B) 103 に送信するという動作を実行する。これによって、仲介装置 (S) 104 は、VPN ゲートウェイ装置 (B) 103 が偽装されていない場合に限り、VPN クライアント装置 (A) 101 に割り当てられた IP アドレス IPADDRESS\_A、及び、共通鍵 KEY\_AB を VPN ゲートウェイ装置 (B) 103 に送信できる。従って、VPN クライアント装置 (A) 101 は、正しい VPN ゲートウェイ装置 (B) 103 を介して、通信装置 (C) 104 と IPsec トンネルモードによるリモ



ートアクセスVPNを実行できるという効果が得られる。

#### 【0060】

また、本実施例において、仲介装置 (S) 104 は、VPNゲートウェイ装置 (B) 103 を認証し、認証に成功した場合に限り、VPNクライアント装置 (A) 101 に割り当てられたIPアドレスIPADDRESS\_A、及び、共通鍵KEY\_ABをVPNゲートウェイ装置 (B) 103 に送信するという動作において、仲介装置 (S) 104 とVPNゲートウェイ装置 (B) 103 との間の通信を暗号化するという動作を実行する。これによって、仲介装置 (S) 104 は、VPNクライアント装置 (A) 101 に割り当てられたIPアドレスIPADDRESS\_A、及び、共通鍵KEY\_ABをすべて改ざんされることなく、かつ、盗聴されることなくVPNゲートウェイ装置Bに送信できる。従って、VPNゲートウェイ装置 (B) 103、及び、通信装置 (C) 111 は、正しいVPNクライアント装置 (A) 101 と、IPsecトンネルモードによるリモートアクセスVPNを実行できる。

#### 【0061】

また、本実施例において、仲介装置 (S) 104 は、SPKI方式に従って、VPNクライアント装置 (A) 101、及び、VPNゲートウェイ装置 (B) 103 を認証すると。これによって、署名確認による本人性証明が可能のため、VPNクライアント装置 (A) 101、及び、VPNゲートウェイ装置 (B) 103 の両者とも仲介装置 (S) 104 に公開鍵証明書を送信する必要がなくなる。従って、VPNクライアント装置 (A) 101 の個人情報もVPNゲートウェイ装置 (B) 103 の個人情報の両者を仲介装置Sに対して隠蔽できる。

#### 【0062】

また、本実施例において、VPNクライアント装置 (A) 101 は、SPKI方式に従って証明書CERTを発行し、VPNクライアント装置 (D) 102 に送信する。これによって、VPNクライアント装置 (A) 101 は、VPNクライアント装置 (D) 102 に対して、VPNゲートウェイ装置 (B) 103 に割り当てられたIPアドレスIPADDRESS\_Bを検索する権限を委譲できるため、VPNクライアント装置 (D) 102、VPNゲートウェイ装置 (B) 103 に割り当てられたIPアドレスIPADDRESS\_Bを検索することができる。かつ、通信装置 (C) 111 に割り当てられたプライベートIPアドレスIPADDRESS\_Cを知ることができる。従って、VPNクライアント装置 (D) 102 も、VPNゲートウェイ装置 (B) 103 を介して通信装置 (C) 111 とIPsecトンネルモードによるリモートアクセスVPNを実行できるという効果が得られる。また、これによって、VPNゲートウェイ装置 (B) 103 は他のVPNクライアント装置 (D) 102 についての情報をアクセスコントロールリスト (ACL) に追加する必要なく、他のVPNクライアント装置 (D) 102 からのリモートアクセスVPNを許可することができる。従って、VPNゲートウェイ装置 (B) 103 は、アクセスコントロールリスト (ACL) の編集などの管理作業に要するコストを軽減できる。

#### 【0063】

なお、図1、図2に示すドメインネームサーバ (DNS) 105において、公開鍵PUBLICKEY\_Bのハッシュ値HASH\_BとIPADDRESS\_Bを関連付けて管理する場合、VPNゲートウェイ装置 (B) 103 は公開鍵PUBLICKEY\_Bのハッシュ値HASH\_Bを生成してから、ハッシュ値HASH\_BとIPアドレスIPADDRESS\_BをドメインネームサーバDNSに登録し、かつ、図4に示す手順 (ステップ1102) を、公開鍵PUBLICKEY\_Bの任意のハッシュ演算アルゴリズムによるハッシュ値HASH\_Bを含むDNSクエリQUERYに変更することにより明らかに実施できる。

#### 【0064】

また、図6に示すアクセスコントロールリスト (ACL)、図7に示すデータTAG、図8に示す演算結果のデータDATA、及び、図9に示す証明書CERTにおいて、SHA-1アルゴリズムの他の任意のハッシュ演算アルゴリズムを用いてハッシュ値HASH\_Aを演算してもよい。また、issuerフィールドの値をハッシュ値HASH\_Aの代わりに公開鍵PUBLICKEY\_Aであると定義してもよい。同様に、subjectフィールドの値をハッシュ値HASH\_Dの代わりに公開鍵PUBLICKEY\_Dと定義してもよい。本変更を実施しても、SPKIに関する非特許文献2及び非特許文献3において定義される演算規則に従って演算することにより、アクセス制御に関して等しい実行結果が得られる。SHA-1アルゴリズム以外のハッシュ演算アルゴリズムを用い

る場合の証明書CERTの形式、及び、issuerフィールド及びsubjectフィールドに公開鍵を指定する場合のアクセスコントロールリストACL、データDATA、及び、証明書CERTの形式については、SPKIに関する非特許文献3において詳細に説明されているため、その詳細な説明については省略する。本変更に伴い、図5に示す手順(ステップ1209)を公開鍵PUBLICKEY\_Aを提示してアクセスコントロールリストACLを検索し、ACLエントリENTRYを取得する手順に変更することにより明らかに実施できる。

#### 【0065】

また、図2に示すVPNクライアント装置(A)101にはグローバルIPアドレスIPADDRESS\_Aのみを割り当てているが、これに加えて、仲介装置(S)104において、非特許文献1に示す方法等を用いてローカルエリアネットワークLAN内の任意のプライベートIPアドレスも割り当てても良い。

#### 【実施例2】

#### 【0066】

本実施例は、証明書CERTについてさらに工夫し、証明書CERTをX.509形式の公開鍵証明書としたものである。基本的なシステム構成は先の実施例1と同様であるが、認証局が必要である。図10に本実施例の全体的システム構成を示す。図10において、VPNクライアント装置(A)101、VPNゲートウェイ装置(B)103、認証局(CA)106、ドメインネームサーバ(DNS)105、及び、仲介装置(S)104はいずれもIP(Internet Protocol)に従ってネットワーク(WAN)100に接続されている。また、通信装置(C)111はVPNゲートウェイ装置(B)103をゲートウェイ装置とするローカルエリアネットワーク(LAN)110に接続されてる。

#### 【0067】

図11は、図10の全体の動作を説明するための図である。太線はIPsecトンネルモードによるリモートアクセスVPN、点線はIKEフェーズ1における認証において、認証局(CA)106に公開鍵証明書CERTを提示することを示している。ここでも、VPNクライアント装置(A)101のホスト名は公開鍵PUBLICKEY\_A(またはそのハッシュ値HASH-A)、IPアドレスはIPADDRESS\_A、VPNゲートウェイ装置(B)103のホスト名は公開鍵PUBLICKEY\_B(またはハッシュ値HASH-B)、IPアドレスはIPADDRESS\_B、または、通信装置(C)111のプライベートIPアドレスはIPADDRESS\_Cとする。

#### 【0068】

VPNクライアント装置(A)101に割り当てられたIPアドレスIPADDRESS\_A、及び、VPNゲートウェイ装置(B)103に割り当てられたIPアドレスIPADDRESS\_BはいずれもIPネットワーク(WAN)100内で一意であり、任意の手段で動的に割り当てられる。VPNゲートウェイ装置(B)103の公開鍵PUBLICKEY\_B(またはHASH-B)とIPアドレスIPADDRESS\_Bはドメインネームサーバ(DNS)105において一意に関連付けて管理される。通信装置(C)111に割り当てられたプライベートIPアドレスIPADDRESS\_Cはローカルエリアネットワーク(LAN)110においてのみ一意であり、DHCP(Dynamic Host Configuration Protocol)、IPCP(PPP IP control protocol)等の任意の手段を用いて動的に割り当てられる。

#### 【0069】

VPNクライアント装置(A)101、VPNゲートウェイ装置(B)103、及び、仲介装置(S)104は、いずれも、IPsecトランスポートモード、または、IPsecトンネルモードにより通信路を暗号化する手段を有する。公開鍵PUBLICKEY\_Aの秘密鍵はPRIVATEKEY\_Aで、VPNクライアント装置(A)101で保管される。CERT\_Aは、秘密鍵PRIVATEKEY\_Aと対となる公開鍵PUBLICKEY\_Aを含むX.509形式の公開鍵証明書で、認証局(CA)106の秘密鍵PRIVATEKEY\_Sで署名され、VPNクライアント装置(A)101で保管される。また、公開鍵PUBLICKEY\_Bの秘密鍵PRIVATEKEY\_Bは、VPNゲートウェイ装置(B)103で保管される。CERT\_Bは、秘密鍵PRIVATEKEY\_Bと対となる公開鍵PUBLICKEY\_Bを含むX.509形式の公開鍵証明書で、同じく認証局(CA)106の秘密鍵PRIVATEKEY\_Sで署名され、VPNゲートウェイ装置(B)103で保管される。認証局(CA)106は、PKI(Public Key Infrastructure)

ure) 方式に従い、VPNクライアント装置 (A) 101の公開鍵証明書CERT\_A、及び、VPNゲートウェイ装置 (B) 103の公開鍵証明書CERT\_Bを認証する。また、アクセスコントロールリスト (ACL) は公開鍵PUBLICKEY\_AとプライベートIPアドレスIPADDRESS\_Cを関連付けたデータで、VPNゲートウェイ装置 (B) 103で保管される。また、秘密鍵PRIVATEKEY\_Sは、仲介装置 (S) 106で保管される。CERT\_Sは、秘密鍵PRIVATEKEY\_Sと対となる公開鍵PUBLICKEY\_Sを含むX. 509形式の公開鍵証明書で、認証局 (CA) 106の秘密鍵で署名され、仲介装置 (S) 104で保管される。

#### 【0070】

仲介装置 (S) 104は (1) VPNゲートウェイ装置 (B) 103の公開鍵PUBLICKEY\_Bをドメインネームサーバ (DNS) 105に提示して、VPNゲートウェイ装置 (B) 103に割り当てられたIPアドレスIPADDRESS\_Bを取得する手段、(2) VPNゲートウェイ装置 (B) 103で保管されるアクセスコントロールリスト (ACL) を記憶する手段、(3) アクセスコントロールリスト (ACL) を参照してアクセス権限制御を実行する手段、及び、(4) 共通鍵KEY\_ABを生成する手段を具備している。上記 (1) に示す手段は、DNS方式と呼ばれるインターネットにおける一般的な名前解決方式に従って、公開鍵PUBLICKEY\_BからIPアドレスIPADDRESS\_Bを解決する。また、上記 (2) に示す手段は、公開鍵PUBLICKEY\_Bと関連付けてアクセスコントロールリスト (ACL) を管理する。また、上記 (3) に示す手段は、公開鍵証明書CERT\_Aに含まれる公開鍵PUBLICKEY\_AをアクセスコントロールリストACLに提示して検索し、検索結果として、公開鍵PUBLICKEY\_Aと一意に関連付けられたプライベートIPアドレスIPADDRESS\_Cを出力する。また、上記 (4) に示す手段は、VPNクライアント装置 (A) 101とVPNゲートウェイ装置 (B) 103との間のIKEフェーズ1における認証に用いる共通鍵KEY\_ABを生成する。

#### 【0071】

次に、図11を参照して、図10の動作概要を説明する。

アクセスコントロール (ACL) の登録(記憶)時、VPNゲートウェイ装置 (B) 103は、公開鍵PUBLICKEY\_B (またはそのHASH-B) とアクセスコントロール (ACL) を仲介装置 (S) 104に送信する(ステップ21)。仲介装置 (S) は該公開鍵PUBLICKEY\_B (またはそのHASH-B) と関連付けてアクセスコントロール (ACL) を記憶する。VPNゲートウェイ装置 (B) 103を経由して、VPNクライアント装置 (A) 101から通信装置 (C) 111にIPsecトンネルモードによるリモートアクセスVPNを実行する場合、VPNクライアント装置 (A) 101は、公開鍵PUBLICKEY\_Aと公開鍵PUBLICKEY\_B (またはそのHASH-B) を仲介装置 (S) 104に送信して、VPNゲートウェイ装置 (B) 103及び通信装置 (C) IPアドレスの検索要求を行なう(ステップ22)。

#### 【0072】

仲介装置 (S) 104は、PKI方式に従ってVPNクライアント装置 (A) 101のアクセス権限制御を実行し、アクセスを許可する場合には、ドメインネームサーバ (DNS) 105を検索してVPNゲートウェイ装置 (B) 103に割り当てられたIPアドレスIPADDRESS\_Bを取得する(ステップ23)。また、仲介 (S) 104は、アクセスコントロール (ACL) を参照して、VPNゲートウェイ装置 (B) 103により管理されるLAN110に接続された通信装置 (C) 111に割り当てられたプライベートIPアドレスIPADDRESS\_Cを取得する。さらに、仲介装置 (S) 104は、VPNクライアント装置 (A) 101との間の認証に用いる共通鍵KEY\_ABを生成する。そして、仲介装置 (S) 104は、仲介装置 (S) 104とVPNクライアント装置 (A) 101との間の通信路を暗号化し、VPNクライアント装置 (A) 101へIPADDRESS\_B、IPADDRESS\_C及び共通鍵KEY\_ABを送信する(ステップ24)。また、仲介装置 (S) 104は、仲介装置 (S) 104とVPNゲートウェイ装置 (B) 103との間の通信路を暗号化し、VPNゲートウェイ装置 (B) 103へIPADDRESS\_AとKEY\_ABを送信する(ステップ25)。

#### 【0073】

以上、図10に示すシステムの各装置の構成及び全体の動作概要を述べたが、ドメインネームサーバ (DNS) 105におけるIPアドレスの管理及び名前解決方法、及び、IPsecトランスポートモードまたはトンネルモードによる通信路の暗号化方法、共通鍵KEY\_ABの生

成方法、及び、PKI方式によるX. 509形式の公開鍵証明書CERT\_A及びCERT\_Bの認証方式については、当業者にとってよく知られているので、その詳細な構成は省略する。

【0074】

以下に、本実施例2におけるアクセスコントロールリスト(ACL)の記憶手順、及びIPアドレスの取得、共通鍵の生成、これらIPアドレスと共通鍵の送信手順について詳述する。

【0075】

まず、図12及び図13を参照して、VPNゲートウェイ装置(B)103において保管されるアクセスコントロールリスト(ACL)を仲介装置(S)104に記憶する手順について説明する。

図12において、VPNゲートウェイ装置(B)103と仲介装置(S)104は、IPsecトランスポートモードにより接続する(ステップ1301)。IKEフェーズ1における認証はPKI方式に従い、VPNゲートウェイ装置(B)103は公開鍵証明書CERT\_Bを送信し、仲介装置(S)104は公開鍵証明書CERT\_Sを送信する。VPNゲートウェイ装置(B)103は受信した公開鍵証明書CERT\_Sを認証局(CA)106に問い合わせ、公開鍵証明書CERT\_Sの正しさをPKI方式に従って認証する。同様に、仲介装置(S)104は受信した公開鍵証明書CERT\_Bを認証局CAに問い合わせ、公開鍵証明書CERT\_Bの正しさをPKI方式に従って認証する。

【0076】

VPNゲートウェイ装置(B)103は、ステップ1301において暗号化された通信路を用いて、アクセスコントロールリスト(ACL)をすべて送信する(ステップ1302)。仲介装置(S)104は、VPNゲートウェイ装置(B)103から送信されたアクセスコントロールリスト(ACL)を登録する(ステップ1303)。その後、VPNゲートウェイ装置(B)103と仲介装置(S)104は、接続を切断する(ステップ1304)。

【0077】

図13は仲介装置(S)104でのアクセスコントロールリスト(ACL)の登録手順の詳細フローである。仲介装置(S)104は、まずVPNゲートウェイ装置(B)103から送信されたアクセスコントロールリスト(ACL)をすべて受信する(ステップ1401)。次に、先のステップ1301におけるIKE認証で用いた公開鍵証明書CERT\_Bを参照して、公開鍵PUBLICKEY\_Bを取得する(ステップ1402)。次に、この取得した公開鍵PUBLICKEY\_Bとステップ1401で受信したアクセスコントロールリストACLを関連づけて記憶する(ステップ1403)。

【0078】

次に、図14及び図15を参照して、仲介装置(S)104が、VPNクライアント装置(A)101とVPNゲートウェイ装置(B)103との間の共通鍵KEY\_ABを生成し、VPNゲートウェイ装置(B)103に割り当てられたIPアドレスIPADDRESS\_B、通信装置(C)111に割り当てられたプライベートIPアドレスIPADDRESS\_C、及び、共通鍵KEY\_ABをVPNクライアント装置(A)101に送信し、また、VPNクライアント装置(A)101に割り当てられたIPアドレスIPADDRESS\_A、及び、共通鍵KEY\_ABをVPNゲートウェイ装置(B)103に送信する手順について説明する。

【0079】

図14において、VPNクライアント装置(A)101と仲介装置(S)104は、IPsecトランスポートモードにより接続する(ステップ1501)。IKEフェーズ1における認証はPKI方式に従い、VPNクライアント装置(A)101は公開鍵証明書CERT\_Aを送信し、仲介装置(S)104は公開鍵証明書CERT\_Sを送信する。VPNクライアント装置(A)101は受信した公開鍵証明書CERT\_Sを認証局(CA)106に問い合わせ、公開鍵証明書CERT\_Sの正しさをPKI方式に従って認証する。同様に、仲介装置(S)104は受信した公開鍵証明書CERT\_Aを認証局(CA)106に問い合わせ、公開鍵証明書CERT\_Aの正しさをPKI方式に従って認証する。

【0080】

VPNクライアント装置(A)101は、ステップ1501において暗号化された通信路を用いて、VPNゲートウェイ装置(B)103の公開鍵PUBLICKEY\_Bを含むDNSクエリQUERYをすべて送信する(ステップ1502)。仲介装置(S)104は、VPNクライアント装置(A)101に割り当てられたIPアドレスIPADDRESS\_A、VPNゲートウェイ装置(B)103に割り当てられたIPアドレスにIPアドレスIPADDRESS\_B、VPNゲートウェイ装置(B)103により管理されるLAN110に接続される通信装置(C)111に割り当てられたプライベートIPアドレスIPADDRESS\_Cを取得し

、VPNクライアント装置 (A) 101とVPNゲートウェイ装置 (B) 103との間のIKE等の認証に用いる共通鍵KEY-ABを生成する(ステップ1503)。図15はステップ1503の詳細処理フローである。

#### 【0081】

図15において、仲介装置(S)104は、まず、VPNクライアント装置 (A) 101から送信されたDNSクエリQUERYをすべて受信して入力する(ステップ1601)。次に、入力したDNSクエリQUERYを参照して、公開鍵PUBLICKEY\_Bをすべて取得する(ステップ1602)。次に、取得した公開鍵PUBLICKEY\_Bをもとに、それに関連付けられたアクセスコントロールリスト (ACL) をすべて取得する(ステップ63)。次に、先のステップ1501におけるIKEフェーズ1認証に用いた公開鍵証明書CERT\_Aを参照して、公開鍵PUBLICKEY\_Aをすべて取得する(ステップ1604)。次に、この取得した公開鍵PUBLICKEY\_Aをもとにアクセスコントロールリスト (ACL) を検索し、プライベートIPアドレスIPADDRESS\_Cを取得する(ステップ1605)。そして、プライベートIPアドレスIPADDRESS\_Cが取得されたと判定し(ステップ1606)、いかなるIPアドレスも取得できない場合には終了する。

#### 【0082】

プライベートIPアドレスIPADDRESS\_Cが取得されたなら、次に、仲介装置Sは、上記ステップ1601において受信したDNSクエリQUERYをドメインネームサーバ(DNS)105に提示して、IPアドレスIPADDRESS\_Bを取得する(ステップ1607)。VPNクライアント装置AのIPアドレスIPADDRESS\_Aを取得する(ステップ1608)。共通鍵KEY\_ABを生成する(ステップ1609)。

#### 【0083】

図14に戻り、仲介装置(S)104は、ステップ1501において暗号化された通信路を用いて、ステップ1607で取得したIPアドレスIPADDRESS\_B、ステップ1605で取得したプライベートIPアドレスIPADDRESS\_C、及び、ステップ1609で生成した共通鍵KEY-ABをすべてVPNクライアント装置(A)101に送信する(ステップ1504)。次に、VPNクライアント装置(A)101と仲介装置(S)104は、接続を切断する(ステップ1505)。

#### 【0084】

次に、VPNゲートウェイ装置 (B) 103と仲介装置(S)104は、IPsecトランスポートモードにより接続する(ステップ1506)。IKEフェーズ1における認証はPKI方式に従い、VPNゲートウェイ装置(B)103は公開鍵証明書CERT\_Bを送信し、仲介装置Sは公開鍵証明書CERT\_Sを送信する。VPNゲートウェイ装置(B)103は、受信した公開鍵証明書CERT\_Sを認証局(CA)106に問い合わせ、公開鍵証明書CERT\_Sの正しさをPKI方式に従って認証する。同様に、仲介装置(S)104は、受信した公開鍵証明書CERT\_Bを認証局(CA)106に問い合わせ、公開鍵証明書CERT\_Bの正しさをPKI方式に従って認証する。

#### 【0085】

仲介装置(S)104は、ステップ1506において暗号化された通信路を用いて、先のステップ1608において取得したIPアドレスIPADDRESS\_A、及び、先のステップ1609において生成した共通鍵KEY\_ABをすべてVPNゲートウェイ装置(B)103に送信する(ステップ1507)。VPNゲートウェイ装置(B)103と仲介装置(S)104は、接続を切断する(ステップ1508)。

#### 【0086】

以上述べたように、本実施例において、仲介装置(S)104は、VPNゲートウェイ装置(B)103より送信された、通信装置(C)111に割り当てられたプライベートIPアドレスIPADDRESS\_Cを記憶することで、仲介装置(S)104は、VPNゲートウェイ装置(B)103だけが知っている、ローカルエリアネットワーク(LAN)に接続された通信装置(C)111に割り当てられたプライベートIPアドレスIPADDRESS\_Cを知ることができる。従って、VPNクライアント装置(A)101は、VPNゲートウェイ装置(B)103を介した通信装置(C)111へのIPsecトンネルモードによるリモートアクセスVPNに必要なプライベートIPアドレスIPADDRESS\_Cを、リモートアクセスVPNを実行する前に仲介装置(S)104に問い合わせることにより知ることができる。

#### 【0087】

また、本実施例において、仲介装置(S)104は、共通鍵KEY\_ABを生成し、生成した共通鍵KEY\_ABをVPNクライアント装置(A)101とVPNゲートウェイ装置(B)103の両者に送信するこれによって、VPNクライアント装置(A)101とVPNゲートウェイ装置(B)103はともに共通鍵KEY\_ABを受信できる。従って、VPNクライアント装置(A)101とVPNゲートウェイ装置(B)103はIKEフェーズ1における認証に用いる共通鍵KEY\_ABをオンラインで共有できる。

#### 【0088】

また、本実施例において、仲介装置(S)104は、VPNゲートウェイ装置(B)103を認証し、認証に成功した場合に限り、VPNゲートウェイ装置(B)103より送信された、通信装置(C)111に割り当てられたプライベートIPアドレスIPADDRESS\_Cを、仲介装置(S)104に記憶する。これによって、仲介装置(S)104は、偽装されていないVPNゲートウェイ装置(B)103から送信されたプライベートIPアドレスIPADDRESS\_Cに限り記憶できる。従って、VPNクライアント装置(A)101は、正しいVPNゲートウェイ装置(B)103から送信されたプライベートIPアドレスIPADDRESS\_Cを知ることができる。

#### 【0089】

また、本実施例において、仲介装置(S)104は、VPNゲートウェイ装置(B)103を認証し、認証に成功した場合に限り、VPNゲートウェイ装置(B)103より送信された、通信装置(C)101に割り当てられたプライベートIPアドレスIPADDRESS\_Cを、仲介装置(S)104に記憶するという動作において、仲介装置(S)104とVPNゲートウェイ装置(B)103との間の通信を暗号化する。これによって、仲介装置(S)104は、VPNゲートウェイ装置(B)103から送信された、通信装置(C)111に割り当てられたプライベートIPアドレスIPADDRESS\_Cを改ざんされことなく、かつ、盗聴されことなく受信できる。従って、VPNクライアント装置(A)101は、正しいVPNゲートウェイ装置(B)103から送信された、通信装置(C)111に割り当てられた正しいプライベートIPアドレスIPADDRESS\_Cを知ることができるという効果が得られる。また、VPNゲートウェイ装置(B)103は、通信装置(C)111に割り当てられた正しいプライベートIPアドレスIPADDRESS\_Cを不特定多数に知られることなく仲介装置(S)104に送信できる。

#### 【0090】

また、本実施例において、仲介装置(S)104は、VPNクライアント装置(A)101を認証し、認証に成功した場合に限り、VPNゲートウェイ装置(B)103に割り当てられたIPアドレスIPADDRESS\_Bをドメインネームサーバ(DNS)105に問い合わせ取得し、共通鍵KEY\_ABを生成し、取得したIPアドレスIPADDRESS\_B、通信装置(C)111に割り当てられたIPアドレスIPADDRESS\_B、及び、生成した共通鍵KEY\_ABをすべてVPNクライアント装置(A)101に送信する。これによって、仲介装置(S)104は、VPNクライアント装置(A)101が偽装されていない場合に限り、VPNゲートウェイ装置(B)103に割り当てられたIPアドレスIPADDRESS\_B、通信装置(C)111に割り当てられたプライベートIPアドレスIPADDRESS\_C、及び、共通鍵KEY\_ABのすべてをVPNクライアント装置(A)101に送信できる。従って、正しいVPNクライアント装置(A)101に限り、VPNゲートウェイ装置(B)103を介して、通信装置(C)111とIPsecトンネルモードによるリモートアクセスVPNを実行できる。

#### 【0091】

また、本実施例において、仲介装置(S)104は、VPNクライアント装置(A)101がVPNゲートウェイ装置(B)103に割り当てられたIPアドレスIPADDRESS\_Bを検索する権限を有しているか否かを判定し、権限を有している場合に限り、VPNゲートウェイ装置(B)103に割り当てられたIPアドレスIPADDRESS\_Bをドメインネームサーバ(DNS)105に問い合わせ取得し、共通鍵KEY\_ABを生成し、取得したIPアドレスIPADDRESS\_B、通信装置(C)111に割り当てられたIPアドレスIPADDRESS\_B、及び、生成した共通鍵KEY\_ABをすべてVPNクライアント装置(A)101に送信する。これによって、仲介装置(S)104は、VPNゲートウェイ装置(B)103に割り当てられたIPアドレスIPADDRESS\_B、通信装置(C)111に割り当てられたプライベートIPアドレスIPADDRESS\_C、及び、共通鍵KEY\_ABのすべてを、VPNゲートウェイ装置(B)103、及び、通信装置(C)111に対しあらかじめアクセス権限を有するVPNクライアント装置(A)101だけに送信できる。従って、VPNゲートウェイ装置(B)103、及び、通信装置(C)111に対する、不特



定多数からのIPsecトンネルモードによるリモートアクセスVPNを防止できる。

【0092】

また、本実施例において、仲介装置(S)104は、仲介装置(S)104とVPNクライアント装置(A)101との間の通信を暗号化する。これによって、仲介装置(S)104は、VPNゲートウェイ装置(B)103に割り当てられたIPアドレスIPADDRESS\_B、通信装置(C)111に割り当てられたプライベートIPアドレスIPADDRESS\_C、及び、共通鍵KEY\_ABを改ざんされことなく、かつ、盗聴されことなくVPNクライアント装置(A)に送信できる。従って、VPNクライアント装置(A)101は、正しいVPNゲートウェイ装置(B)103を介して、正しい通信装置(C)111と、IPsecトンネルモードによるリモートアクセスVPNを実行できる。

【0093】

また、本実施例において、仲介装置(S)104は、VPNゲートウェイ装置(B)103を認証し、認証に成功した場合に限り、VPNクライアント装置(A)101に割り当てられたIPアドレスIPADDRESS\_A、及び、共通鍵KEY\_ABをVPNゲートウェイ装置(B)103に送信する。これによって、仲介装置(S)104は、VPNゲートウェイ装置(B)103が偽装されていない場合に限り、VPNクライアント装置(A)101に割り当てられたIPアドレスIPADDRESS\_A、及び、共通鍵KEY\_ABをVPNゲートウェイ装置(B)103に送信できる。従って、VPNクライアント装置Aは、正しいVPNゲートウェイ装置(B)103を介して、通信装置(C)111とIPsecトンネルモードによるリモートアクセスVPNを実行できる。

【0094】

また、本実施例において、仲介装置(S)104は、VPNゲートウェイ装置(B)103を認証し、認証に成功した場合に限り、VPNクライアント装置(A)101に割り当てられたIPアドレスIPADDRESS\_A、及び、共通鍵KEY\_ABをVPNゲートウェイ装置(B)103に送信するという動作において、仲介装置(S)104とVPNゲートウェイ装置(B)103との間の通信を暗号化する。これによって、仲介装置(S)104は、VPNクライアント装置(A)101に割り当てられたIPアドレスIPADDRESS\_A、及び、共通鍵KEY\_ABをすべて改ざんされことなく、かつ、盗聴されことなくVPNゲートウェイ装置(B)103に送信できる。従って、VPNゲートウェイ装置(B)103、及び、通信装置(C)111は、正しいVPNクライアント装置(A)101と、IPsecトンネルモードによるリモートアクセスVPNを実行できる。

【0095】

また、本実施例において、仲介装置(S)104は、PKI方式に従って、VPNクライアント装置(A)101、及び、VPNゲートウェイ装置(B)103を認証する。これによって、VPNクライアント装置(A)101の公開鍵証明書CERT\_AもVPNゲートウェイ装置(B)103の公開鍵証明書CERT\_Bも仲介装置(S)104に送信することにより認証できる。従って、VPNクライアント装置(A)101の個人情報をVPNゲートウェイ装置(B)103に対して隠蔽できる。同様に、VPNゲートウェイ装置(B)103の個人情報をVPNクライアント装置(A)101に対して隠蔽できる。

なお、本実施例における図10、図11に示すドメインネームサーバ(DNS)105において、公開鍵PUBLICKEY\_Bの任意のハッシュ演算アルゴリズムによるハッシュ値HASH\_BとIPADDRESS\_Bを関連付けて管理する場合、VPNゲートウェイ装置(B)102は公開鍵PUBLICKEY\_Bのハッシュ値HASH\_Bを生成してから、ハッシュ値HASH\_BとIPアドレスIPADDRESS\_Bをドメインネームサーバ(DNS)105に登録すればよい。また、図14に示す手順のステップ1502を、公開鍵PUBLICKEY\_Bの任意のハッシュ演算アルゴリズムによるハッシュ値HASH\_Bを含むDNSクエリQUERYに変更することにより明らかに実施できる。

【0096】

また、アクセスコントロールリスト(ACL)において、公開鍵PUBLICKEY\_AとIPアドレスIPADDRESS\_Cを関連付けて管理する代わりに、公開鍵PUBLICKEY\_Aの任意のハッシュ演算アルゴリズムによるハッシュ値HASH\_AとIPアドレスIPADDRESS\_Cと関連付けて管理しても良い、本変更に伴い、図12に示す手順のステップ1302において、VPNゲートウェイ装置(B)103は公開鍵PUBLICKEY\_Aのハッシュ値HASH\_Aを生成してから、ハッシュ値HASH\_AとIPアドレスIPADDRESS\_Cをアクセスコントロールリスト(ACL)として関連付けたデータを送信することにより明らかに実施できる。かつ、図15に示す手順のステップ1605を公開鍵PUBLICKEY

Y\_Aのハッシュ値HASH\_Aを生成し、ハッシュ値HASH\_Aを提示してアクセスコントロールリストACLを検索する手順に変更することにより、明らかに実施できる。

【0097】

また、VPNクライアント装置(A)101にはグローバルIPアドレスIPADDRESS\_Aのみを割り当てているが、これに加えて、仲介装置(S)104において、非特許文献1に示す方法等を用いてローカルエリアネットワークLAN内の任意のプライベートIPアドレスを割り当てても良い。

【0098】

なお、実施例1や実施例2で示したシステムにおける各装置の一部もしくは全部の処理機能をコンピュータのプログラムで構成し、そのプログラムをコンピュータを用いて実行して本発明を実現することができること、あるいは、実施例1や実施例2で示した処理手順をコンピュータのプログラムで構成し、そのプログラムをコンピュータに実行させることができることは言うまでもない。コンピュータでその処理機能を実現するためのプログラム、あるいは、コンピュータにその処理手順を実行させるためのプログラムを、そのコンピュータが読み取り可能な記録媒体、例えば、FD、MO、ROM、メモリカード、CD、DVD、リムーバブルディスクなどに記録して、保存したり、提供したりすることができるとともに、インターネット等のネットワークを通してそのプログラムを配布したりすることが可能である。

【図面の簡単な説明】

【0099】

【図1】本発明の第1の実施例におけるシステム構成例を示す図である。

【図2】本発明の第1の実施例の動作概要を説明する図である。

【図3】本発明の第1の実施例におけるアクセスコントロールACLの記憶手段を示す図である。

【図4】本発明の第1の実施形態におけるIPアドレス及び共通鍵の送信手順を示す図である。

【図5】本発明の第1の実施例における仲介装置でのIPアドレスの取得手順、及び、共通鍵の生成手順の詳細処理フロー図である。

【図6】本発明の第1の実施例におけるアクセスコントロールリストACLの一例である。

【図7】本発明の第1の実施例におけるデータTAGの一例である。

【図8】本発明の第1の実施例における演算結果データDATAの一例である。

【図9】本発明の第1の実施例における証明書CERTの一例である。ネットワークを通してそのプログラムを配布したりすることが可能である。

【図10】本発明の第2の実施例におけるシステム構成例を示す図である。

【図11】本発明の第2の実施例の動作概要を説明する図である。

【図12】本発明の第2の実施例におけるアクセスコントロールACLの記憶手段を示す図である。

【図13】本発明の第2の実施例における仲介装置でのアクセスコントロールリストACLの記憶手順の詳細処理フロー図である。

【図14】本発明の第2の実施例におけるIPアドレス及び共通鍵の配布手順を示す図である。

【図15】本発明の第2の実施例における、仲介装置でのIPアドレスの取得手順、及び、共通鍵の生成手順の詳細処理フロー図である。

【符号の説明】

【0100】

100 IPネットワーク (WAN)

101, 102 VPNクライアント装置

103 VPNゲートウェイ装置

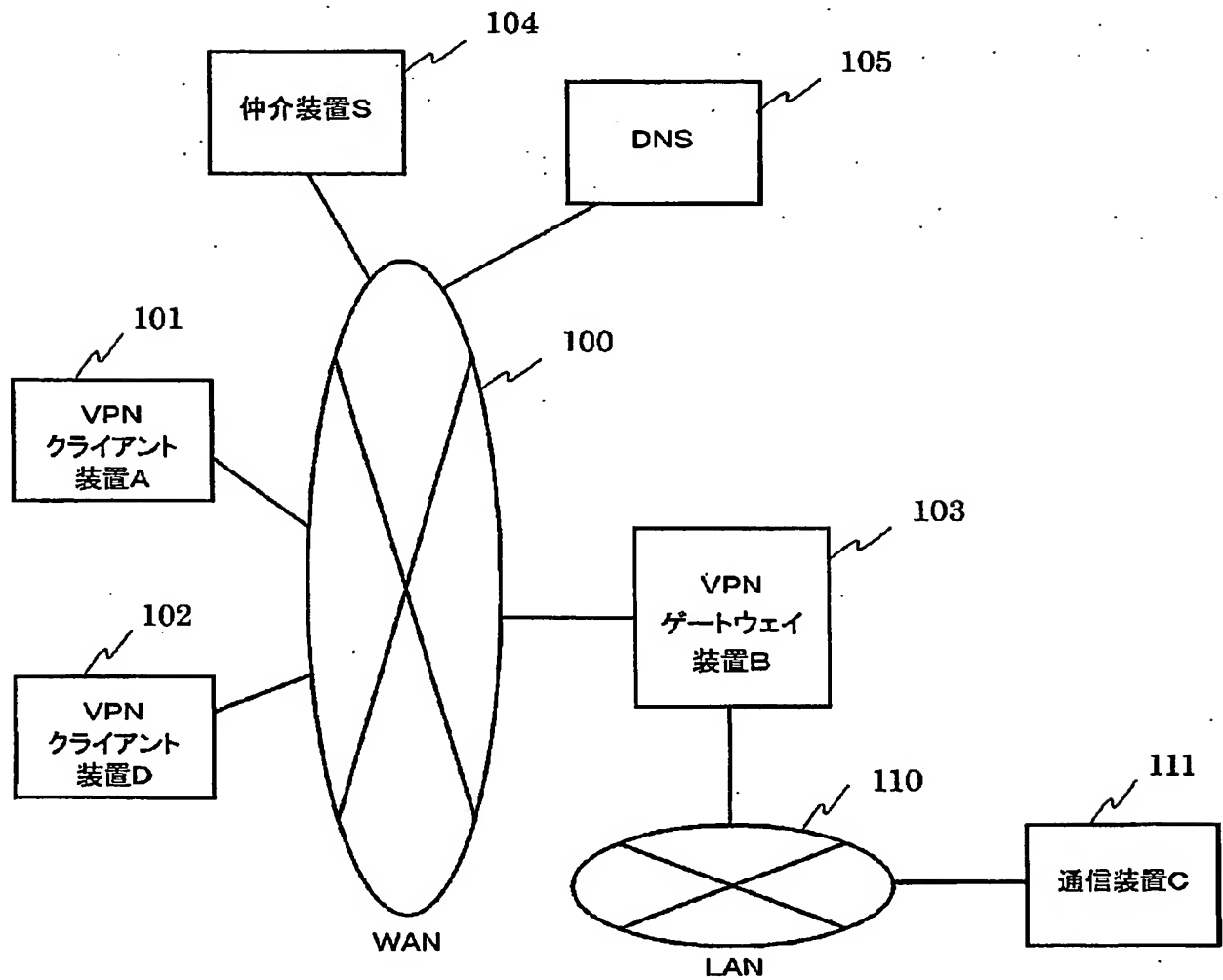
104 仲介装置



- 105 ドメインネームサーバ (DNS)
- 110 ローカルエリアネットワーク (LAN)
- 111 通信装置

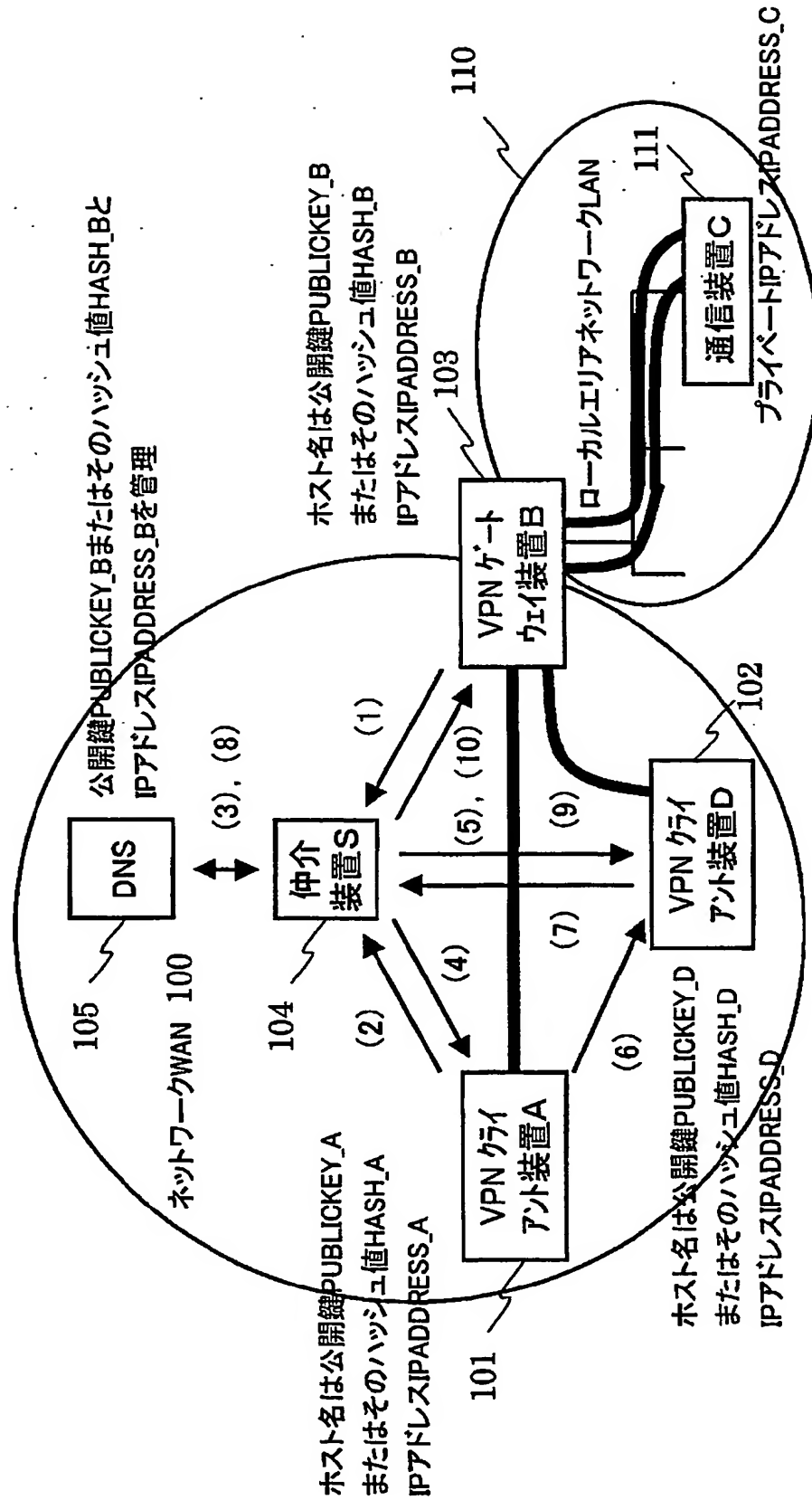
【書類名】 図面  
【図 1】

本発明の第1の実施例のシステム構成例



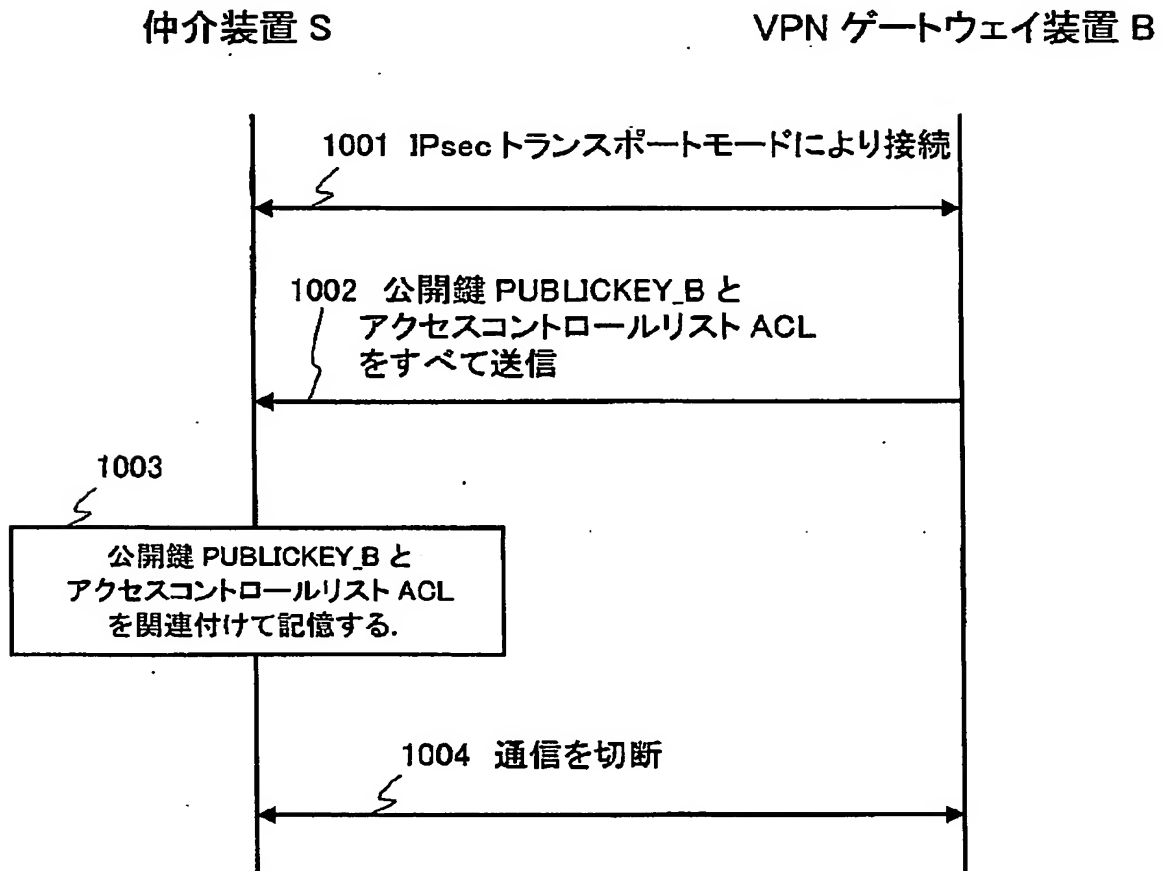
【図2】

## 本発明の第1の実施例の動作概要



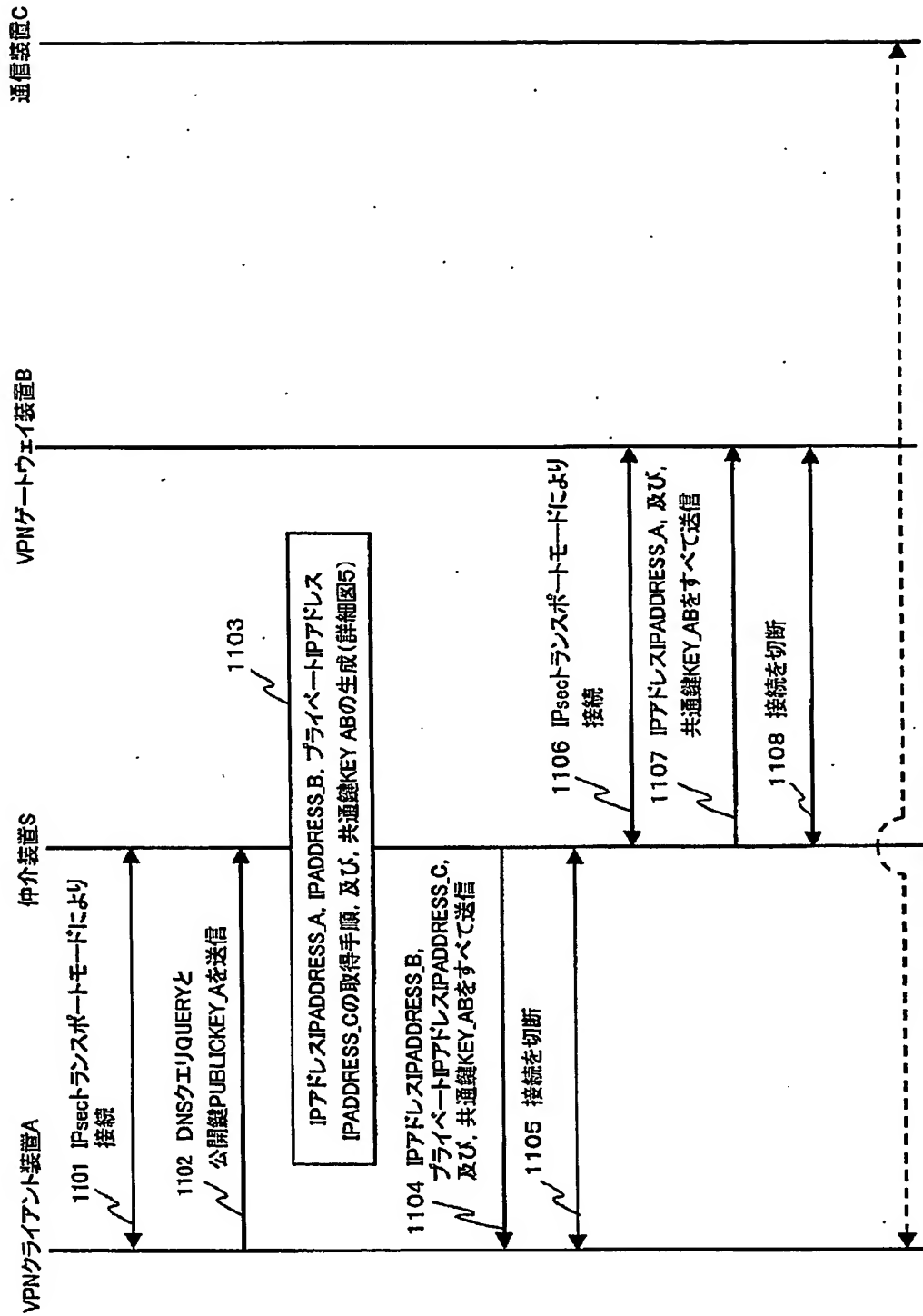
【図 3】

本発明の第1の実施例におけるアクセスコントロールリストACLの記憶手順



【図 4】

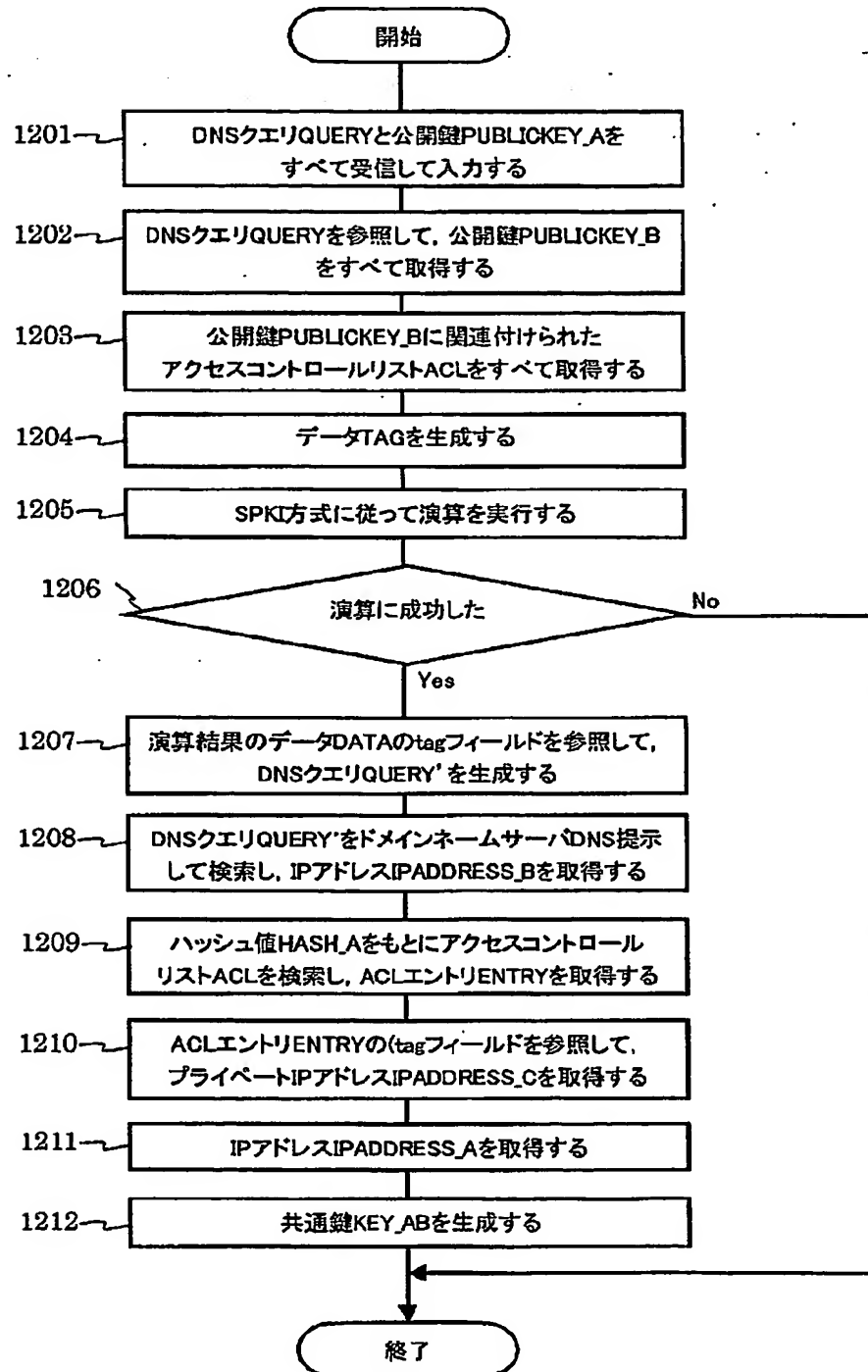
本発明の第1の実施例における IP アドレス IPADDRESS\_A, IP アドレス IPADDRESS\_B,  
プライベート IP アドレス IPADDRESS\_C、および共通鍵 KEY\_AB 送信手順



VPNゲートウェイ装置Bを経由して、VPNクライアント装置Aから通信装置Cに  
IPsecトンネルモードによるリモートアクセスVPNを実行

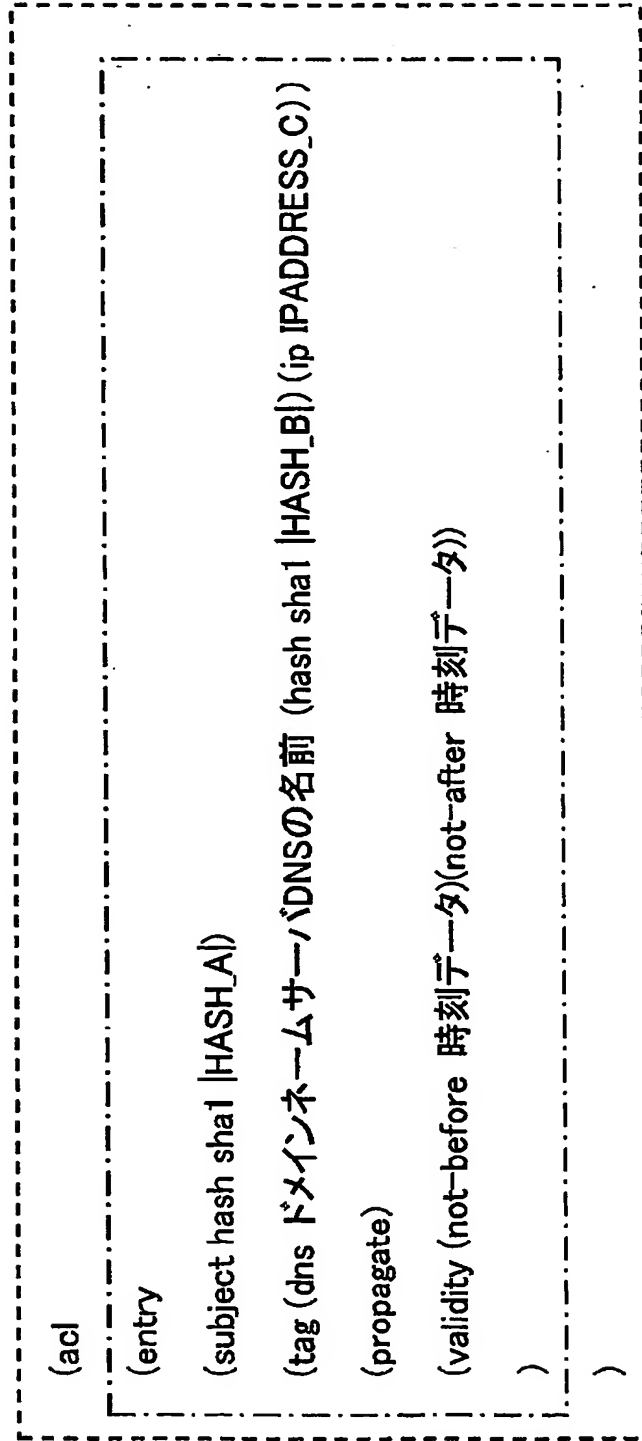
【図 5】

本発明の第1の実施例における IP アドレス IPADDRESS\_A、IP アドレス IPADDRESS\_B、  
プライベート IP アドレス IPADDRESS\_C、の取得手順、および共通鍵 KEY\_AB の生成手順



【図 6】

本発明の第1の実施例におけるアクセスコントロールリストACLの例



アクセスコントロールリストACLとして定義されるデータ

ACLエントリENTRYとして定義されるデータ

【図 7】

## 本発明の第1の実施例におけるデータTAGの例



(tag (dns ドメインネームサーバーバDNSの名前 (hash sha1 |HASH\_B|)))



データTAGとして定義されるデータ

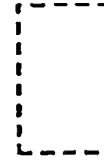


【図 8】

本発明の第1の実施例における演算結果データDATAの例

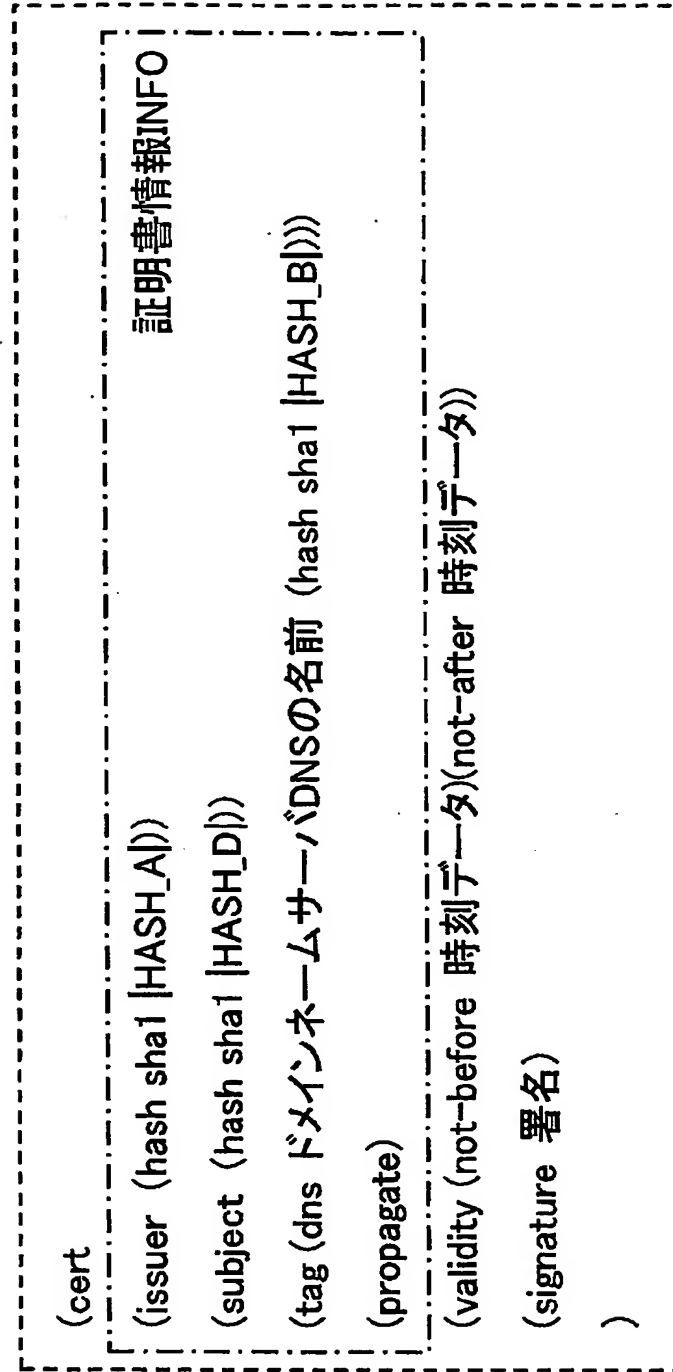
```
(cert
(issuer Self)
(subject (hash sha1 |HASH_A|))
(tag (dns ドメインネームサーバDNSの名前 (hash sha1 |HASH_B|)))
(propagate)
(validity (not-before 時刻データ)(not-after 時刻データ))
)
```

演算結果データDATAとして定義されるデータ



【図 9】

本発明の第1の実施例における証明書CERTの例

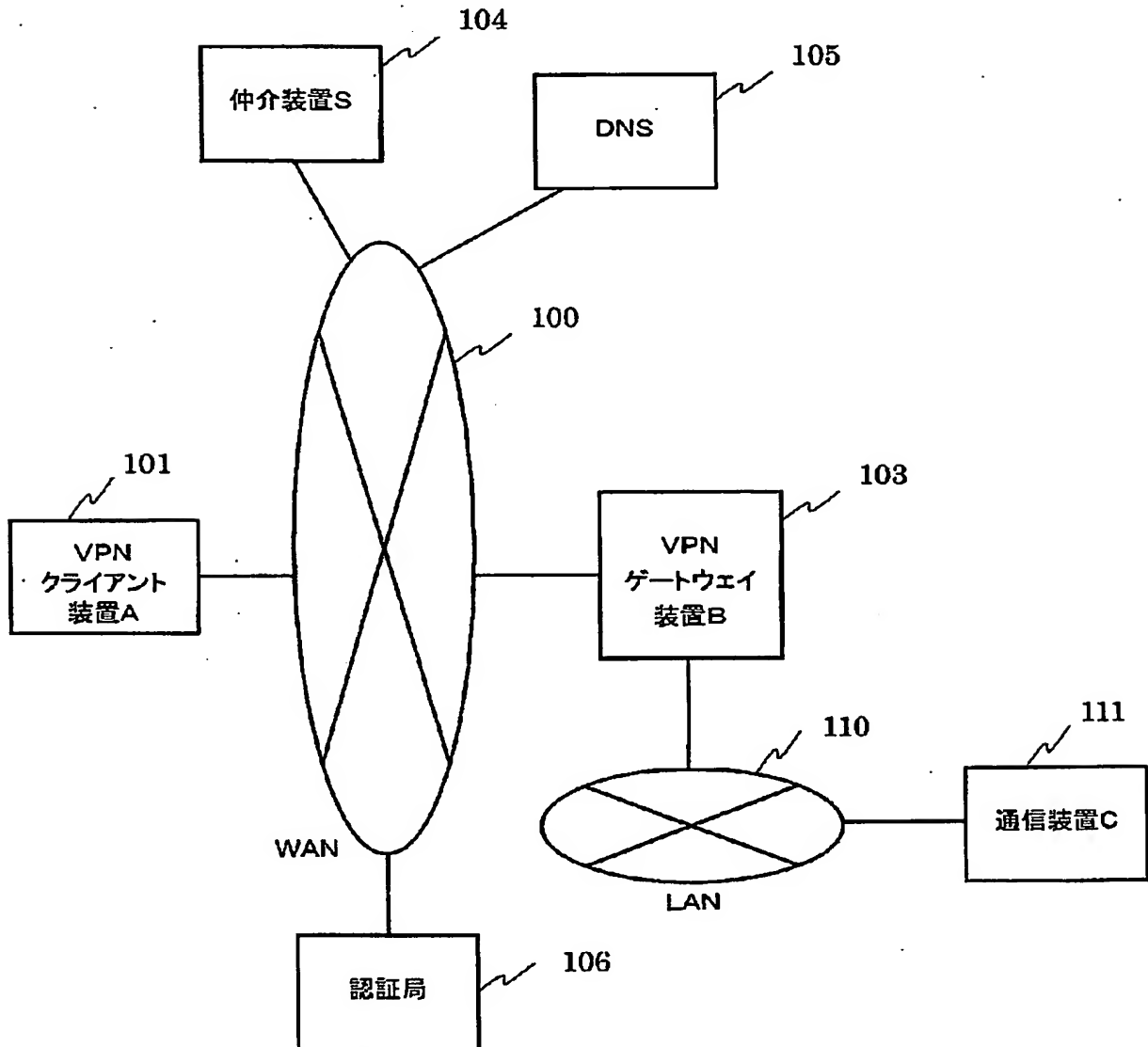


証明書CERTとして定義されるデータ

証明書情報INFOとして定義されるデータ

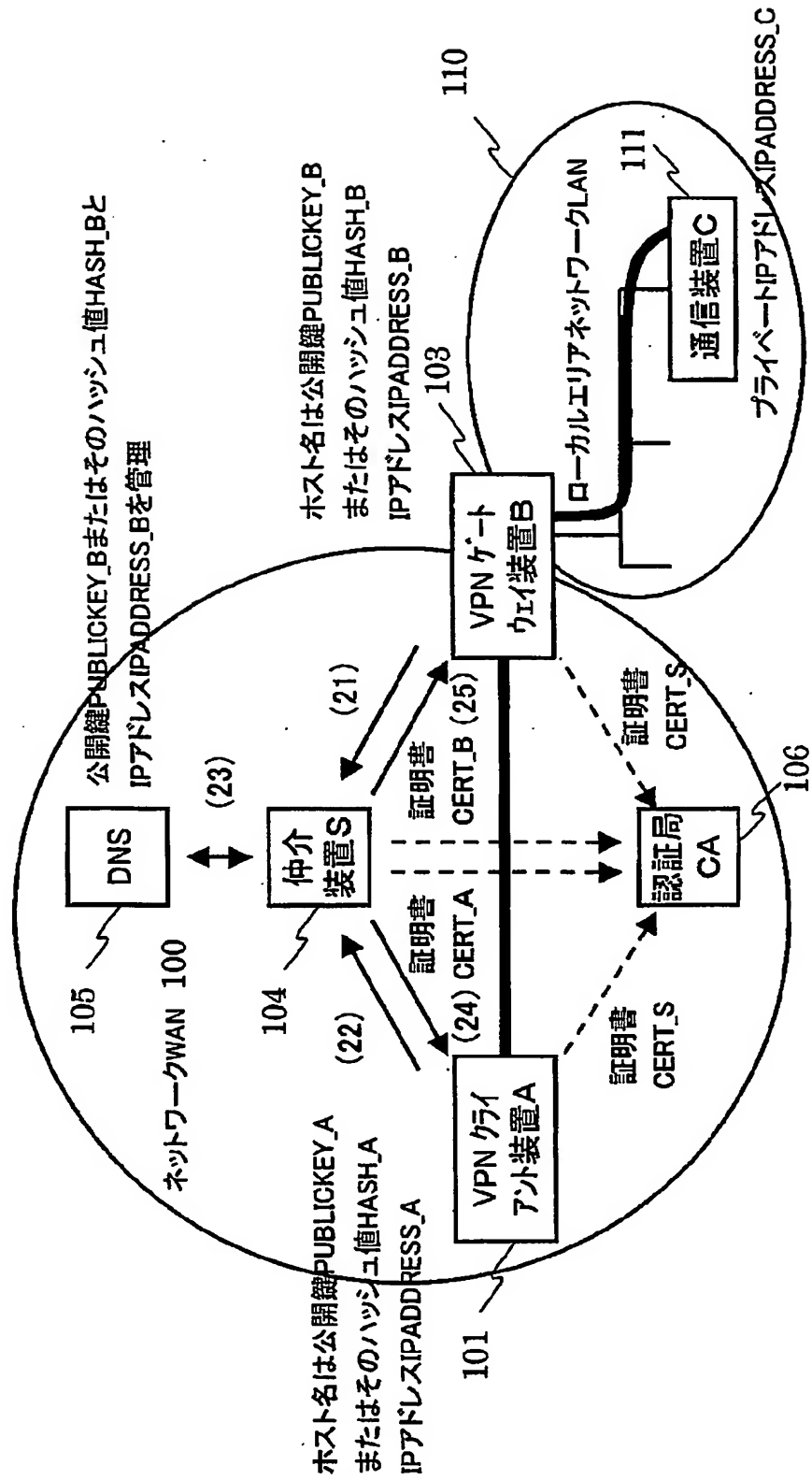
【図10】

## 本発明の第2の実施例のシステム構成例



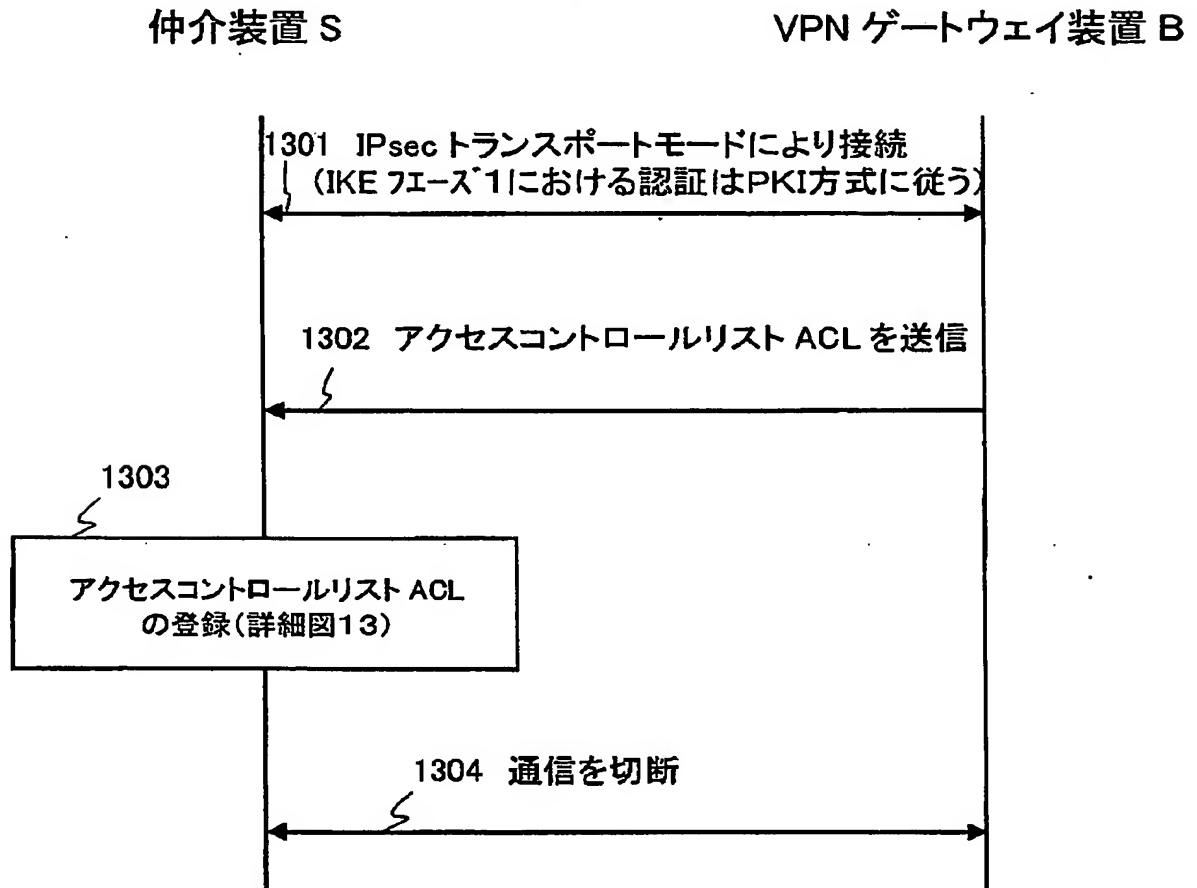
【図11】

本発明の第2の実施例の動作概要



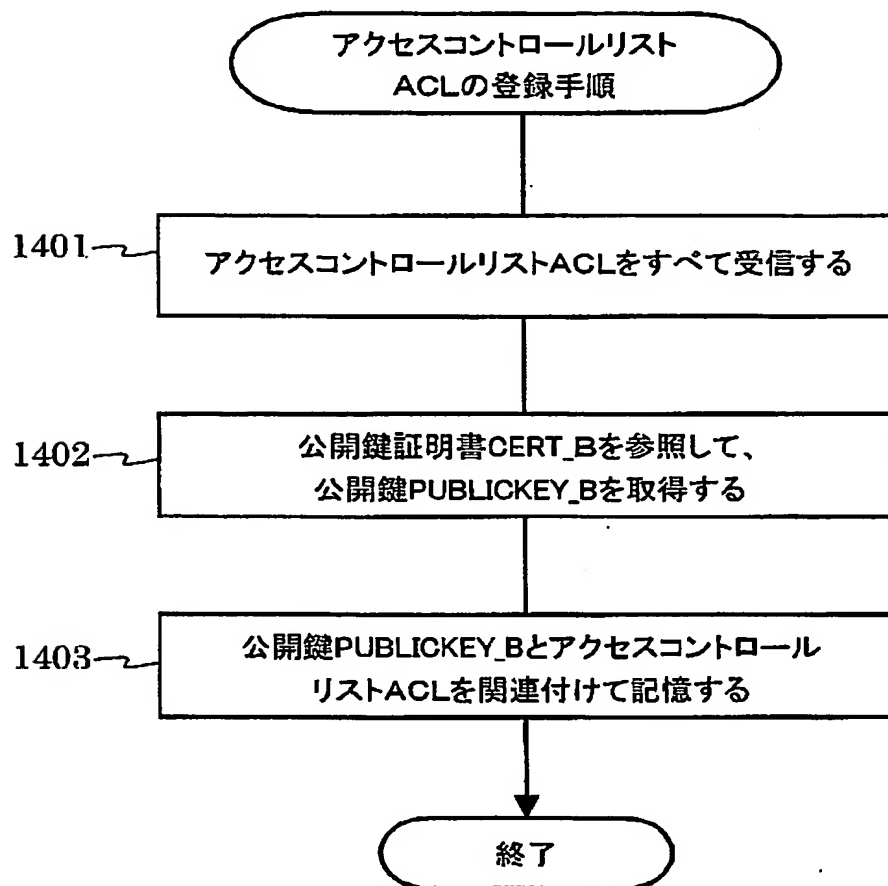
【図 12】

本発明の第2の実施例におけるアクセスコントロールリストACLの記憶手順



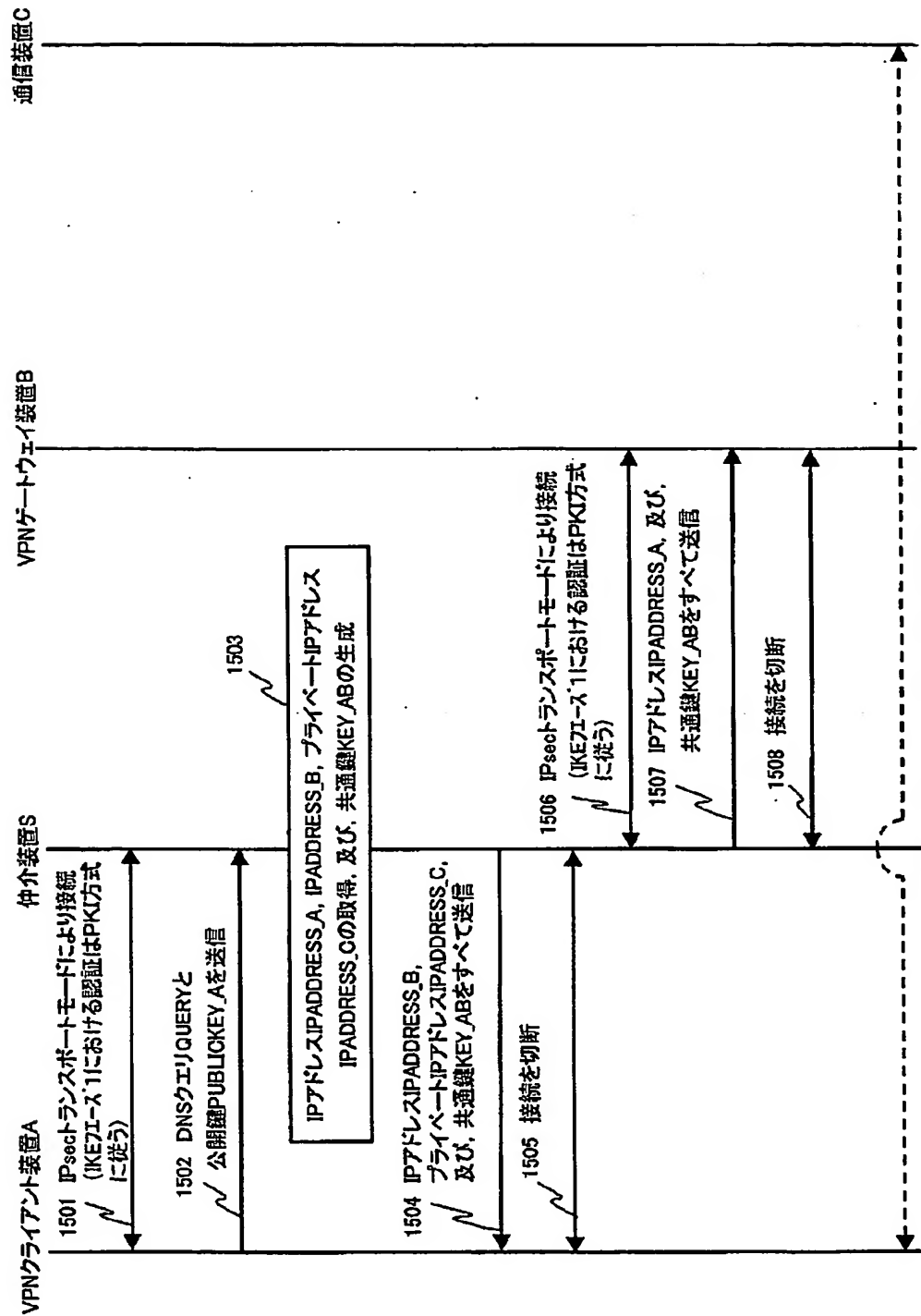
【図13】

本発明の第2の実施例における仲介装置Sにおける  
アクセスコントロールリストACLの記憶手順



【図 14】

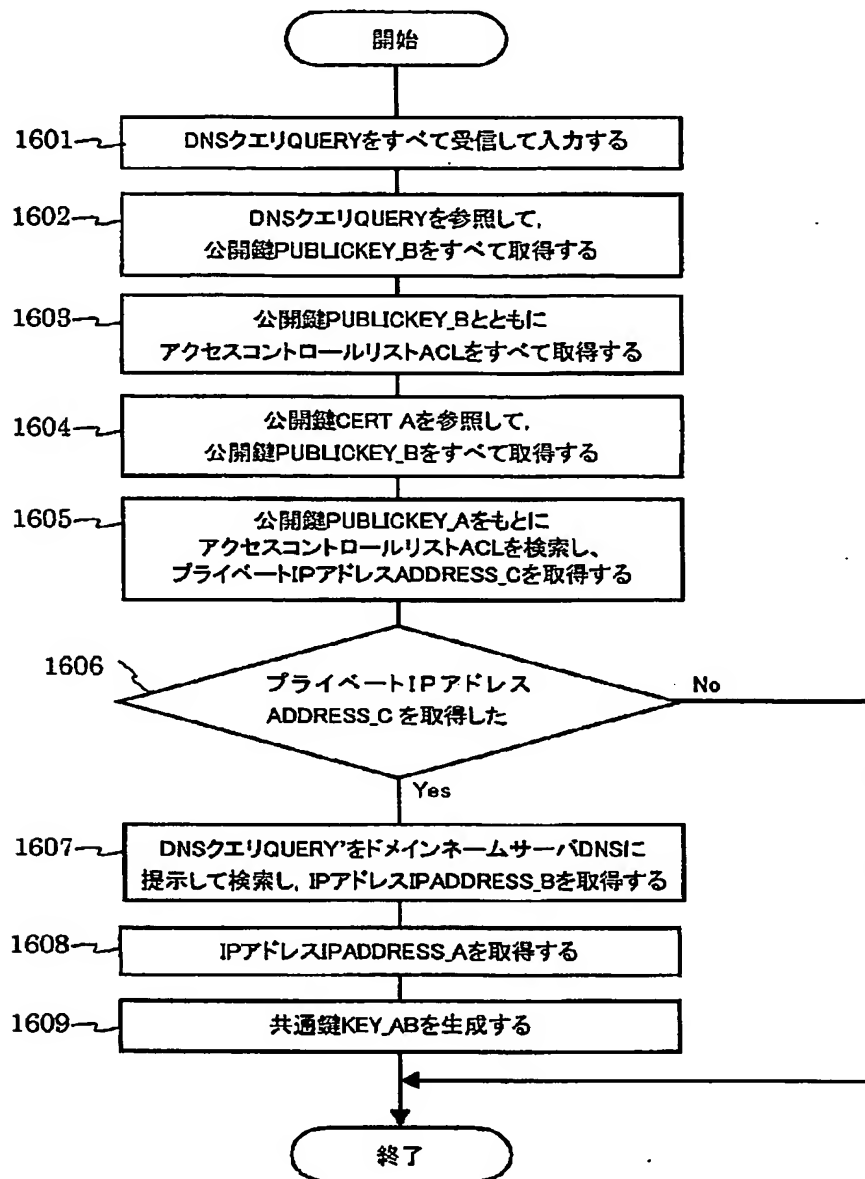
本発明の第2の実施例における IP アドレス IPADDRESS\_A, IP アドレス IPADDRESS\_B,  
プライベート IP アドレス IPADDRESS\_C、および共通鍵 KEY\_AB 送信手順



VPNゲートウェイ装置Bを経由して、VPNクライアント装置Aから通信装置Cに  
IPsecトンネルモードによるリモートアクセスVPNを実行

【図 15】

本発明の第 2 の実施例における IP アドレス IPADDRESS\_A, IP アドレス IPADDRESS\_B, プライベート IP アドレス IPADDRESS\_C、の取得手順、および共通鍵 KEY\_AB の生成手順





**【書類名】 要約書****【要約】**

**【課題】** インターネットにおいて、IPsec等のトンネリングプロトコルによるリモートアクセスVPNを確立するための情報を安全に共有できるようにする。

**【解決手段】** IPネットワーク上に仲介装置を設け、VPNゲートウェイ装置で保管されるアクセスコントロールリスト(ACL)を記憶する。仲介装置は、VPNクライアント装置から検索要求を受信し、ACLを参照して通信装置のプライベートIPアドレスを取得し、DNSを検索してVPNゲートウェイ装置のIPアドレスを取得し、VPNクライアント装置とVPNゲートウェイ装置との間の認証に用いる共通鍵を生成し、VPNゲートウェイ装置のIPアドレス、通信装置のプライベートIPアドレス及び共通鍵をVPNクライアント装置に送信し、VPNクライアント装置のIPアドレス及び共通鍵をVPNゲートウェイ装置に送信する。

**【選択図】** 図2

特願 2 0 0 3 - 2 7 1 2 0 2

出 願 人 履 歴 情 報

識別番号 [ 0 0 0 0 0 4 2 2 6 ]

1. 変更年月日 1 9 9 9 年 7 月 1 5 日

[変更理由] 住所変更

住 所 東京都千代田区大手町二丁目 3 番 1 号

氏 名 日本電信電話株式会社